

SNOW SHOE HUNTING WITH GOLANG



**Trials and Tribulations From the Front Line Support Desk
John Van Lowe (JVL) @ ATX GoLang Feb 2026 Meetup**

The Agenda - Our Training Data For This Talk



- Gratitudes
- whoami
- Snow what?
- Inspiration and Intent

- First Hunts (shell scripted)
- Faster Hunts (with go)
- Campaign Hunt Demo

- What Next?

Gratitudes - Quick Token of Appreciation



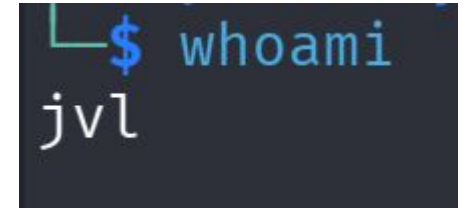
Food & Drinks

Station Austin

Attendees

Whoami - John Van Lowe = JVL

- acba.coop - board member, advisor, chair for housing committee
- bokbot.org - automated chicken coop efforts
- festivalbeach.org - Food Forest on city property
- keepaustinfed.org - Moving millions of pounds of food
- webhosting.coop - applying the consumer coop ownership model to digital services



- Prior NASA JSC MCC FC, USAF F-16 Crew Chief, Micron, Codero...

Snow What? Definition and Risks

Snow Shoe Spamming “a practice that spammers use to send from many IP addresses and domains to avoid being caught by spam filters.”

Why does this matter? Your network reputation dictates the success of businesses that depend on deliverability.



I2C init Sept 2012 - I2Coalition via <https://i2coalition.com/>

SHA init Feb 2025- Secure Hosting Alliance via <https://hostingsecurity.net/>

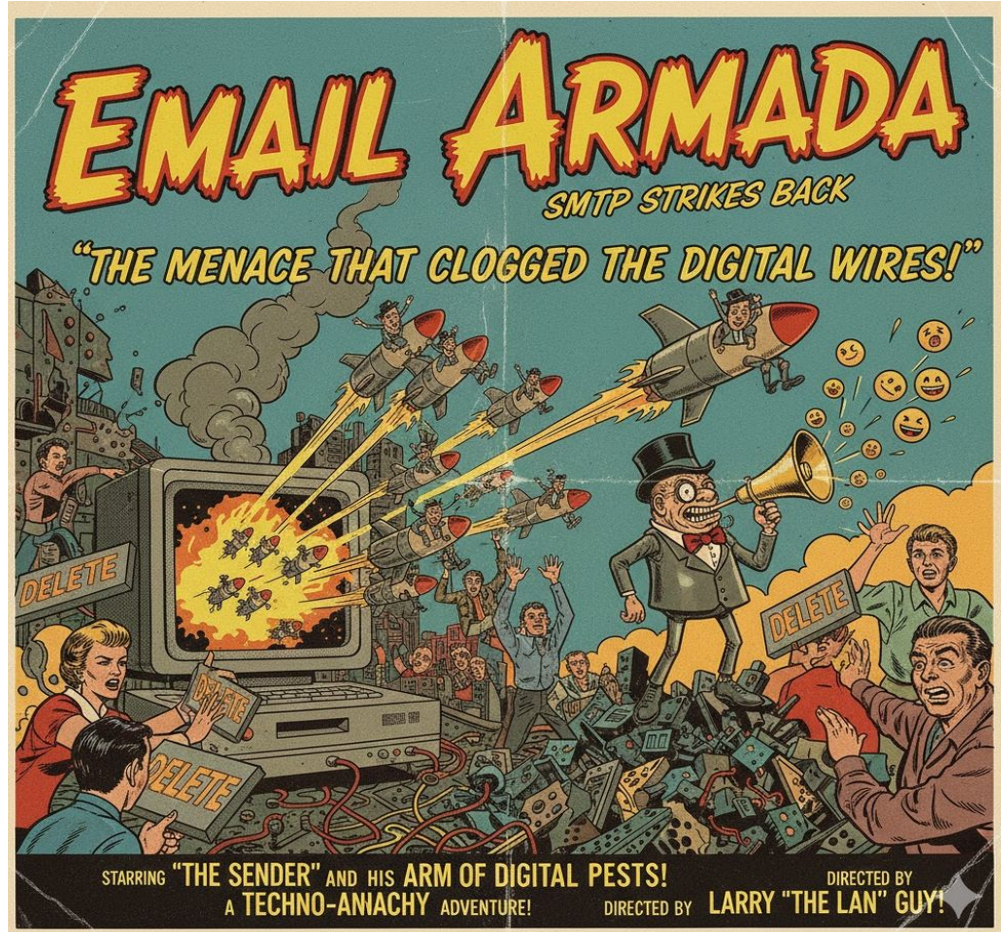
Inspiration and Intent

What inspired this talk?

Jan 2025 ATX GoLang Meet
(chromium),

[VetSec.org](https://www.vetsec.org) discussions
(support group for veterans
working toward a career in
cyber security),

“The 2016 Support Call”.



THE SUPPORT CALL - With the headers

- It was our box
- It was a stateside address
- It had no abuse history
- It had custom PTR records
- It had a deliberate Forward and Reverse DNS Match ***
- It was a name match on ROKSO via SPAMHAUS



THE ABUSE REVIEW - responsible spammers profile

- All servers with ipv4 and PTR support
- CentOS (and then Almalinux)
- SSH port would close after setup and typical mail and web ports would be exposed



- Extensive local /etc/host files (avoid passive DNS monitoring)
- Declared A record, CNAME, and MX records for well know destinations (hotmail, yahoo, gmail, aol).

THE SUSPENSIONS - social engineering

- **Illinois drivers licenses, Moroccan IP first SSH login with root creds**
- **Intermittent DC Signups (billing origin AS)**
- **Addresses for UPS stores and fast food chain locations**
- **Whitelisted C&C infra in Vegas**
 - Blacklisted on edges - obvious in traceroute
 - Added switch ACLs, in troubleshooting they pivoted to...
- **C&C box on another client ID (4 boxes on our AS, the rest at SoftLayer, etc)**
- **“We fixed it” and “Our client sent spam we have talked to them and also installed spam filter”**
- **NEVER a name on the signature of the request**
- **Burn account, last cancel server mail blasting after end date set**
- **Sales / RFQ emails occasionally forget to remove the comments saying do not contact specific providers (liquid web / colo crossing)**
- **Pivot to Ukraine (name, MA IP)**

THE BIGGER PICTURE - how big is this op?

- **Top notch infra monitoring**
- **Alerts for ICMP and service state**
- **Estimated 100 boxes globally.**
- **Realized it was just a single campaign on a single domain**
- **Spamhaus takes down ROKSO publicly. No longer ToS relevant.**
- **Looking for ways to prove ring association without upstream list**



FIRST HUNTS - bash scripting

- A campaign is matched with abbreviation kss.
- The hostnames in the campaign are numerically incremented in order over time. In the campaign servers like kss100 were purchased in 2017, kss1000 hosts were deployed in 2019.
- Shell scripts used to resolve IPs from hostnames, determine if they were alive with ICMP, see if port 25 was open, and lookup the PTR records.

```
#!/bin/bash
THIS_NAME=$1
DIG1=$(dig $THIS_NAME +short|head -n1)
DIG2=$(dig -x $DIG1 +short|head -n1)
PINGS=$(ping -W 7 -c 1 $DIG1> /dev/null 2>/dev/null; echo $? )
echo $THIS_NAME,$PINGS,$DIG1,$DIG2
onehunt (END)
```

Result: Effective but time consuming as the events were sequential. Each portion ICMP, TCP socket connect, etc had another timeout to wait for.

```
#!/bin/bash
TMP=$(mktemp -d --suffix=HUNTER)
PRE_KSS=$(cat PRE_KSS)
POST_KSS=$(cat POST_KSS)
x=$(cat LOWER_NUM)
END=$(cat UPPER_NUM)
echo HOSTNAME,PINGS,IP,PTR > $TMP/diggit.csv
cp onehunt $TMP/onehunt
while [ $x -le $END ]
do
    THIS_NUM=$(printf "%03d" $x)
    THIS_NAME=$(echo $PRE_KSS$THIS_NUM$POST_KSS)
    echo "./onehunt $THIS_NAME >>$TMP/diggit.csv" >> $TMP/working.sh
    x=$(( $x + 1 ))
done

/usr/bin/time parallel --jobs 225 -- < $TMP/working.sh
cp $TMP/diggit.csv ./para-diggit.csv
rm -rf $TMP
```

Faster Hunts - Go tooling! hunt1.go

- Jan 27 flip into golang with help of gemini
- Check A record, PTR, SMTP, latency
- First revision to declare IPs to ignore
 - Wildcard responses from resolvers
 - Indicates Dead Hostname if IP Match

```
[kss975.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 5.97496434s
[kss725.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 5.971687354s
[kss663.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 5.990705434s
[kss184.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.059081841s
[kss221.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.047913596s
[kss330.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.051762595s
[kss716.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.056387712s
[kss288.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.085532367s
[kss139.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.095160823s
[kss373.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.091031024s
[kss922.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.105020417s
[kss642.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.105718091s
[kss354.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.106604987s
[kss388.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.114651578s
[kss541.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.121515613s
[kss131.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.154114057s
[kss544.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.16413988s
[kss285.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.168800762s
[kss584.web.nrb-apps.com] IP: 213.181.109.133 Status: UP Latency: 6.168813766s
```

```
package main

import (
    "encoding/csv"
    "fmt"
    "net"
    "os"
    "sync"
    "time"
)

//
const IgnoredIP = "1.2.3.4"

type HunterResult struct {
    Hostname string
    IP        string
    Status    string
    Latency   string
}

func main() {
    var prefix, suffix string
    var startRange, endRange int

    // 1. User Inputs
    fmt.Println("— KSSHunter Go Refactor (With IP Filter) —")
    fmt.Print("Enter Subdomain Prefix: ")
    fmt.Scanln(&prefix)
    fmt.Print("Enter Domain Suffix: ")
    fmt.Scanln(&suffix)
    fmt.Print("Start Number: ")
    fmt.Scanln(&startRange)
    fmt.Print("End Number: ")
    fmt.Scanln(&endRange)

    // 2. Setup CSV Output
    file, err := os.Create("ksshunter_filtered_results.csv")
    if err != nil {
        fmt.Printf("Error creating CSV: %v\n", err)
        return
    }
    defer file.Close()

    writer := csv.NewWriter(file)
```

Faster Hunts - a few iterations ahead, hunt4.go

- Playing with formatting, reporting if SMTP is up
- Skipping ICMP and jumping straight to SMTP
 - Avoid worrying about user being able to send ICMP
 - One less Response to time out
- If it provides a banner the host is alive

```
(jvl@laptop) - [~/KSShunter]
└─$ go run hunt4.go
└─ KSShunter Go (SMTP Port 25 + PTR Lookup) ─
Enter Subdomain Prefix: css
Enter Domain Suffix: web.nrb-apps.com
Start Number: 1500
End Number: 1600

Hunting targets on Port 25 ... (Ignoring: 213.181.109.133)

[css1571.web.nrb-apps.com] IP: 91.191.208.170 SMTP: UP PTR: aetlimo.com
[css1529.web.nrb-apps.com] IP: 67.23.250.138 SMTP: UP PTR: arielevans.com
[css1563.web.nrb-apps.com] IP: 172.111.9.245 SMTP: UP PTR: returntothebeach.com
[css1500.web.nrb-apps.com] IP: 199.249.171.152 SMTP: UP PTR: maverickincomenow.com
[css1537.web.nrb-apps.com] IP: 178.32.110.244 SMTP: UP PTR: spiralstairsme.com
[css1586.web.nrb-apps.com] IP: 193.161.204.216 SMTP: UP PTR: ophthalmologypc.com
[css1535.web.nrb-apps.com] IP: 199.249.171.239 SMTP: UP PTR: marksenglishschool.com
[css1502.web.nrb-apps.com] IP: 209.236.124.94 SMTP: UP PTR: steelviewmfg.com
[css1600.web.nrb-apps.com] IP: 67.23.237.90 SMTP: UP PTR: saracourtney.com
[css1536.web.nrb-apps.com] IP: 178.32.96.29 SMTP: UP PTR: bestspect.com
[css1503.web.nrb-apps.com] IP: 204.74.215.250 SMTP: UP PTR: prolegacyfoundation.com
[css1528.web.nrb-apps.com] IP: 184.171.249.90 SMTP: UP PTR: thatsrome-bb.com
[css1556.web.nrb-apps.com] IP: 69.166.8.100 SMTP: UP PTR: raisingrowers.com
[css1566.web.nrb-apps.com] IP: 142.171.159.138 SMTP: UP PTR: clqcb.com
[css1592.web.nrb-apps.com] IP: 199.249.171.19 SMTP: UP PTR: hamblemotors.com
[css1594.web.nrb-apps.com] IP: 212.24.177.226 SMTP: UP PTR: manlyweekend.com
[css1588.web.nrb-apps.com] IP: 204.74.211.2 SMTP: Down PTR: N/A
```

Faster Hunts - show me both IPs, hunt5.go

- Showing both the resolved IP and PTR IP
- The match is the single most important metric many providers use to determine if your mail should be delivered
- It is impossible to have a match without deliberate actions in both zones

```
(jvl@laptop) [~/KSShunter]
$ go run hunt5.go
— KSShunter Go (Port 25 + PTR Double-Check) —
Enter Subdomain Prefix: css
Enter Domain Suffix: web.nrb-apps.com
Start Number: 1600
End Number: 1700
[+] Presentation Found...

Hunting ... (Filtering: 213.181.109.133)

HOSTNAME                INITIAL IP      SMTP    PTR RECORD                PTR IP
-----
css1601.web.nrb-apps.com 67.23.237.114  UP      kittycatbeautyshop.com    67.23.237.114
css1611.web.nrb-apps.com 67.23.234.170  UP      ishanyeresin.com          67.23.234.170
css1610.web.nrb-apps.com 84.16.240.138  UP      304area.com                84.16.240.138
css1691.web.nrb-apps.com 184.154.202.162 UP      pamelamalunat.com         184.154.202.162
css1689.web.nrb-apps.com 172.245.209.87 UP      quantumleapresources.com   172.245.209.87
css1600.web.nrb-apps.com 67.23.237.90   UP      saracourtney.com           67.23.237.90
css1620.web.nrb-apps.com 178.162.194.83 UP      brucetphillipslaw.com     178.162.194.83
css1650.web.nrb-apps.com 67.23.231.186  UP      4zube.com                   67.23.231.186
css1649.web.nrb-apps.com 67.23.231.194  UP      notoriousstires.com        67.23.231.194
css1634.web.nrb-apps.com 95.214.55.61   UP      go2keys.com                 95.214.55.61
css1604.web.nrb-apps.com 51.79.22.182   UP      andrewpoulsen.com          51.79.22.182
css1624.web.nrb-apps.com 67.23.233.74   UP      ryanbuckingham.com         67.23.233.74
```

Faster Hunts - PTR + banner match, hunt6.go

- Showing the SMTP banner with the PTR records
- The banner is set in the MTA config on the host, the PTR is set at the provider via whatever means they are exposing records to clients (WHMCS, ubersmith, netbox, etc)

```
(jvl@laptop) - [~/KSShunter]
$ go run hunt6.go
--- KSShunter Go (SMTP Banner + PTR Validation) ---
Enter Subdomain Prefix: css
Enter Domain Suffix: web.nrb-apps.com
Start Number: 1600
End Number: 1700

Hunting ... (Filtering: 213.181.109.133)
```

HOSTNAME	IP	SMTP	BANNER	PTR RECORD
css1601.web.nrb-apps.com	67.23.237.114	UP	220 kittycatbeautyshop.co ...	kittycatbeautyshop.com
css1604.web.nrb-apps.com	51.79.22.182	UP	220 andrewpoulsen.com ESM ...	andrewpoulsen.com
css1611.web.nrb-apps.com	67.23.234.170	UP	220 ishanyeresin.com ESMT ...	ishanyeresin.com
css1691.web.nrb-apps.com	184.154.202.162	UP	220 pamelamalunat.com ESM ...	pamelamalunat.com
css1689.web.nrb-apps.com	172.245.209.87	UP	220 quantumleapresources. ...	quantumleapresources.com
css1620.web.nrb-apps.com	178.162.194.83	UP	220 brucetphillipslaw.com ...	brucetphillipslaw.com
css1649.web.nrb-apps.com	67.23.231.194	UP	220 notorioustires.com ES ...	notorioustires.com
css1600.web.nrb-apps.com	67.23.237.90	UP	220 saracourtney.com ESMT ...	saracourtney.com
css1624.web.nrb-apps.com	67.23.233.74	UP	220 ryanbuckingham.com ES ...	ryanbuckingham.com
css1634.web.nrb-apps.com	95.214.55.61	UP	220 go2keys.com ESMT ser ...	go2keys.com
css1650.web.nrb-apps.com	67.23.231.186	UP	220 gotogirlmd.com ESMT ser ...	4zube.com
css1610.web.nrb-apps.com	84.16.240.138	UP	220 304area.com ESMT ser ...	304area.com

Faster Hunts - console + CSV output, hunt10.go

- Use the data in other places from scan_results.csv
- Easy to have additional utilities take the output as separate process
- Skip having screenshot logic in same routine

```
Scanning from css1800.web.nrb-apps.com to css1900.web.nrb-apps.com ...
```

HOSTNAME	IP	PORT 25	PTR RECORD	MATCH?
css1887.web.nrb-apps.com	23.111.154.10	Open	morgarrh.com	Yes
css1862.web.nrb-apps.com	184.154.22.18	Open	meubleschezpierre.com	Yes
css1873.web.nrb-apps.com	192.227.96.90	Open	consteinsac.com	Yes
css1856.web.nrb-apps.com	198.50.158.165	Open	laurenboscia.com	Yes
css1861.web.nrb-apps.com	15.235.123.150	Open	balibisnisweb.com	Yes
css1848.web.nrb-apps.com	148.135.105.242	Open	cmchevy.net	Yes
css1890.web.nrb-apps.com	69.162.103.74	Open	reggente.com	Yes
css1838.web.nrb-apps.com	69.162.106.98	Open	arocare-b-matsuyama.com	Yes
css1900.web.nrb-apps.com	74.63.237.146	Open	chicoullah.com	Yes
css1854.web.nrb-apps.com	172.111.8.158	Open	adamoriti.com	Yes
css1802.web.nrb-apps.com	95.214.52.161	Open	watertanksupply.com	Yes
css1849.web.nrb-apps.com	172.111.10.184	Open	drgregoryjduncan.com	Yes
css1898.web.nrb-apps.com	198.27.89.159	Open	baronvonjager.com	Yes
css1801.web.nrb-apps.com	192.99.114.32	Open	bartech-egypt.com	Yes
css1871.web.nrb-apps.com	199.217.106.120	Open	sportschiromed.com	Yes
css1886.web.nrb-apps.com	208.89.61.141	Open	time.cplusddns.com	Yes
css1858.web.nrb-apps.com	51.89.6.9	Open	tjsexp.com	Yes
css1844.web.nrb-apps.com	149.50.96.7	Open	productionmobile.com	Yes
css1833.web.nrb-apps.com	95.214.53.4	Open	readntick.com	Yes
css1841.web.nrb-apps.com	23.111.155.22	Open	ksmmaintenance.com	Yes
css1885.web.nrb-apps.com	208.89.63.153	Open	inukshukusa.com	Yes
css1853.web.nrb-apps.com	96.127.136.82	Open	b-zukan.com	Yes
css1875.web.nrb-apps.com	69.65.31.22	Open	msclenavi.com	Yes
css1843.web.nrb-apps.com	94.72.166.186	Open	belfastselfstorage.com	No
css1847.web.nrb-apps.com	64.95.98.42	Open	jpvalois.com	Yes
css1842.web.nrb-apps.com	198.50.157.237	Open	forbiddenwhispers.com	Yes
css1899.web.nrb-apps.com	82.131.160.149	Open	oshawasports.com	Yes
css1832.web.nrb-apps.com	95.110.225.95	Open	bookmarkingdemon.org	Yes
css1837.web.nrb-apps.com	185.189.134.116	Open	freejoomla.com	Yes
css1884.web.nrb-apps.com	107.190.135.162	Open	cuddlehealer.com	Yes
css1846.web.nrb-apps.com	148.251.150.176	Open	canal-stream1.com	No

```
Scan Complete. Results saved to scan_results.csv
```

Faster Hunts - Evidence via screenshots.go

- Reading in scan_results.csv
- Creates screenshot of fake unsubscribe pages loading for vhost entry matching the PTR FQDN
- Import chromedp
- Locked up laptop

```
package main

import (
    "context"
    "encoding/csv"
    "fmt"
    "log"
    "os"
    "strings"
    "time"
    "github.com/chromedp/chromedp"
    "github.com/chromedp/cdproto/emulation"
)

// CSV Column Indexes (Based on previous app's output)
// 0: Hostname, 1: IP Address, 2: Port 25, 3: Banner, 4: PTR Record, ...
const (
    ColIP      = 1
    ColPTR     = 4
    OutputFolder = "output"
)

func main() {
    // 1. Setup Output Directory
    if _, err := os.Stat(OutputFolder); os.IsNotExist(err) {
        os.Mkdir(OutputFolder, 0755)
    }

    // 2. Open CSV File
    csvFile, err := os.Open("scan_results.csv")
    if err != nil {
        log.Fatal("Could not open scan_results.csv. Run the previous app first!", err)
    }
    defer csvFile.Close()

    reader := csv.NewReader(csvFile)
    records, err := reader.ReadAll()
    if err != nil {
        log.Fatal("Error reading CSV:", err)
    }

    // 3. Setup Chrome Context
    // We create one allocator to reuse the browser instance for speed
    opts := append(chromedp.DefaultExecAllocatorOptions[:],
        chromedp.Flag("headless", true), // Run without a window
        chromedp.WindowSize(1280, 768), // Set window size explicitly
    )
```

Faster Hunts - Evidence via screenshots200.go

- Creating worker queue to process five at a time
- Ensuring FQDN, IP, and timestamp are in the file name
- Previously a manual task when suspending a box
- Ensuring proper resolution for WindowSize

```
// 3. Setup Chrome
opts := append(chromedp.DefaultExecAllocatorOptions[:],
  chromedp.Flag("headless", true),
  chromedp.Flag("disable-gpu", true),
  chromedp.Flag("ignore-certificate-errors", true),
  chromedp.WindowSize(1280, 768),
)

allocCtx, cancel := chromedp.NewExecAllocator(context.Background(), opts...)
defer cancel()

ctx, cancel := chromedp.NewContext(allocCtx)
defer cancel()

if err := chromedp.Run(ctx); err != nil {
  log.Fatal("Could not start browser:", err)
}

// 4. Worker Pool Setup
jobs := make(chan Job, len(records))
var wg sync.WaitGroup

fmt.Printf("Starting %d workers (HTTP Check + Screenshot) ... \n", WorkerCount)
for w := 1; w ≤ WorkerCount; w++ {
  wg.Add(1)
  go worker(w, ctx, jobs, &wg)
}
}
```

Faster Hunts - IP to ASN Mapping

- Using geoip2-golang
- Public Max Mind ASN .mmdb from github
- Combined with ips.csv reports ASN
- Sorts and shows count per provider

```
    "github.com/oschwald/geoip2-golang"
)

// Result holds the data for a single IP lookup
type Result struct {
    IP      string
    ASN     uint
    Org     string
}

func main() {
    db, err := geoip2.Open("GeoLite2-ASN.mmdb")
    if err != nil {
        log.Fatalf("Error opening database: %v", err)
    }
    defer db.Close()

    file, err := os.Open("ips.csv")
    if err != nil {
        log.Fatalf("Error opening ips.csv: %v", err)
    }
}
```

185.164.138.63	AS62240	Clouvider Limited
185.164.139.90	AS62240	Clouvider Limited
185.164.139.109	AS62240	Clouvider Limited
103.75.71.162	AS62390	NexonHost Srl
176.126.84.236	AS63473	HostHatch, LLC
103.199.103.250	AS138195	MOACK.Co.LTD
23.82.137.21	AS393886	Leaseweb USA, Inc.
23.19.44.168	AS395954	Leaseweb USA, Inc.
198.135.49.99	AS396073	Majestic Hosting Solutions,

### Total Counts Per Provider ###		
Organization		Count
OVH SAS		15
Leaseweb USA, Inc.		9
Internap Holding LLC		9
Clouvider Limited		6
HostDime.com, Inc.		5
Limestone Networks, Inc.		5
GigeNET		4
Think BV Limited		4
Leaseweb Deutschland GmbH		3
WorldStream B.V.		3
GloboTech Communications		2
Scalaxy B.V.		2
FREE RANGE CLOUD - Free Range Cloud Hosting Inc.		2
WIIT AG		1
Savvy s.r.o.		1
velia.net Internetdienste GmbH		1
Hostwinds LLC.		1
HostHatch, LLC		1
Leaseweb Canada Inc.		1
Contabo GmbH		1
LeaseWeb Netherlands B.V.		1
Informacines sistemas ir technologijos, UAB		1
MOACK.Co.LTD		1
Orange		1
Majestic Hosting Solutions, LLC		1
IONOS SE		1

Campaign Hunt Demo - css*

- Run a hostname block scan to .csv
- Screenshot records
- All are either blank 404 not found page or content with a fake unsubscribe page
- The submit button changes the dom to say thanks for unsub but never posts

```
(jvl@laptop)-[~/KSShunter]
└─$ go run hunt10.go
┌─ Advanced Network Scanner (A + PTR + FCrDNS + SMTP) ─┐
Enter subdomain prefix (e.g., 'mail'): css
Enter domain suffix (e.g., 'example.com'): web.nrb-apps.com
Enter start value (numeric): 1000
Enter stop value (numeric): 1100

Scanning from css1000.web.nrb-apps.com to css1100.web.nrb-apps.com ...

┌──────────┬──────────┬──────────┬──────────┬──────────┐
│ HOSTNAME  │ IP        │ PORT 25  │ PTR RECORD │ MATCH?    │
├──────────┴──────────┴──────────┴──────────┴──────────┘
css1010.web.nrb-apps.com 198.49.67.90 Open generationsalaam.com Yes
css1008.web.nrb-apps.com 138.128.171.138 Open snyderbilt.com Yes

Scan Complete. Results saved to scan_results.csv

(jvl@laptop)-[~/KSShunter]
└─$ go run goscreenshots.go
Starting 15 workers to process screenshots...
[Worker 7] Processing: generationsalaam.com
[Worker 1] Processing: snyderbilt.com

Processing complete. 2 screenshots attempted.

(jvl@laptop)-[~/KSShunter]
└─$ ls -l output/
total 24
12 -rw-r--r-- 1 jvl jvl 10989 Feb 10 21:29 snyderbilt.com_138.128.171.138_2026-02-10.png
12 -rw-r--r-- 1 jvl jvl 10989 Feb 10 21:29 generationsalaam.com_198.49.67.90_2026-02-10.png
```

Campaign Hunt Demo - Hunt + Screenshots live

- Resolvers willing...
 - Enumerate 10000 records from css campaign
- Gather screenshot evidence
- Review ASN Data
- Discuss

oshawasp	pamelama	partynavi	philipooli	plasticsurg	polirip.co	powerlines	AS33182	HostDime.com, Inc.	24
orts.com	lunat.com	om_184.15	n.com_91.	erythai.co	m_184.154	poetry.co	AS32475	Internap Holding LLC	21
82.131.160	184.154.20	4.202.82_	221.70.75_	m_23.111.1	.135.122_2	m_69.175.	AS16276	OVH SAS	12
.149_2026	2.162_202	2026-02-1	2026-02-1	70.26_202	026-02-10	22.250_20	AS174	Cogent Communications, LLC	11
-02-10.png	6-02-10.p	0.png	0.png	6-02-10.p	.png	26-02-10.	AS201814	MEVSPACE sp. z o.o.	10
	ng			ng		png	AS33083	AxcelX Technologies LLC	10
							AS46475	Limestone Networks, Inc.	9
							AS29802	HIVELOCITY, Inc.	7
							AS20248	Take 2 Hosting, Inc.	4
							AS30277	DFW Datacenter	4
							AS12301	Invitech ICT Services Kft.	3
production	prolegacyf	quantumle	raisingrow	readntick.c	redpalmsv	reggente.c	AS35916	MULTACOM CORPORATION	3
mobile.co	oundation.	apresourc	ers.com_6	om_95.214	illa.com_1	om_69.16	AS14315	1GSERVERS, LLC	3
m_149.50	com_204.	es.com_17	9.166.8.10	.53.4_202	41.95.211.1	2.103.74_2	AS51783	The Center of Dedicated Servers LLC	3
96.7_2026	74.215.250	2.245.209.	0_2026-0	6-02-10.p	66_2026-	026-02-10	AS64236	UnReal Servers, LLC	3
-02-10.png	_2026-02-	87_2026-	2-10.png	ng	02-10.png	.png	AS24940	Hetzner Online GmbH	2
	10.png	02-10.png					AS32181	Gigamon	2
							AS28753	Leaseweb Deutschland GmbH	2
							AS63513	Sia Nano IT	2
							AS31034	Aruba S.p.A.	2
							AS13886	Cloud South	2
returntoth	richardsau	ryanbuckin	saracourtn	slidersima	snyderbilt.	sptruckin	AS400773	Boston Fiber LLC	1
ebeach.co	tomotive.n	gham.com	ey.com_67	ges.com_1	com_138.1	g.com_184	AS63018	Dedicated.com	1
m_172.111.	et_95.214.	_67.23.233	_23.237.90	49.50.126.	28.171.138	.154.219.2	AS396073	Majestic Hosting Solutions, LLC	1
9.245_202	55.60_202	.74_2026-	_2026-02-	57_2026-0	_2026-02-	42_2026-	AS51167	Contabo GmbH	1
6-02-10.p	6-02-10.p	02-10.png	10.png	2-10.png	10.png	02-10.png	AS63023	GTHost	1
ng	ng						AS30633	Leaseweb USA, Inc.	1
							AS55154	Madgenius.com	1
							AS40279	ForestRacks	1
							AS51765	Oy Crea Nova Hosting Solution Ltd	1
spiralstair	sportschir	sslwebmai	steelview	takehomek	thatsrome	time.cplus	AS35908	Krypt Technologies	1
sme.com	omed.com	l.com_136.	mfg.com_	arate.com	-	ddns.com_	AS27956	Cyber Cast International, S.A.	1
178.32.110.	_199.217.1	175.11.218	209.236.1	_190.97.16	bb.com_18	208.89.61.	AS26042	FiberState, LLC	1
244_2026	06.120_20	2026-02-1	24.94_202	5.182_202	4.171.249.	141_2026-	AS54600	PEG TECH INC	1
-02-10.png	26-02-10.	0.png	6-02-10.p	6-02-10.p	90_2026-	02-10.png	AS7203	Leaseweb USA, Inc.	1
							AS36352	HostPapa	1

Next Steps?

- Convert all inputs into command line flags or pull from environment variables
- Handle Context deadline exceeded
- Handle ERR_NAME_NOT_RESOLVED

- **Clean up this presentation and present to the SHA**
- **Create a reporting mechanism to send notifications to appropriate hosts.**
- **Determine who will care if I don't have headers?**
- **Discuss further on Gopher Slack!?**