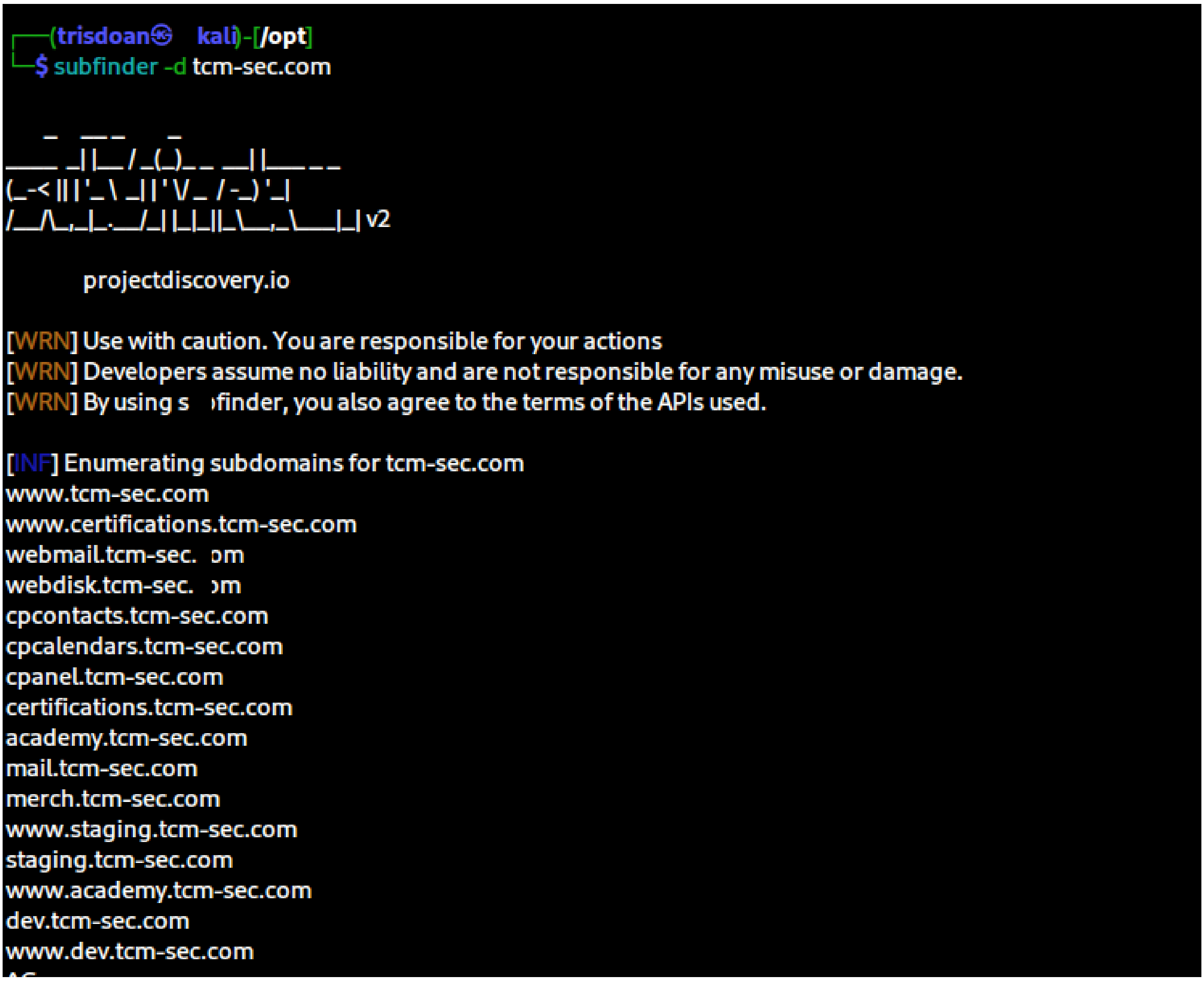
WEBSITE OSINT

TOOLS:

WAPPALIZER (ON FIREFOX)

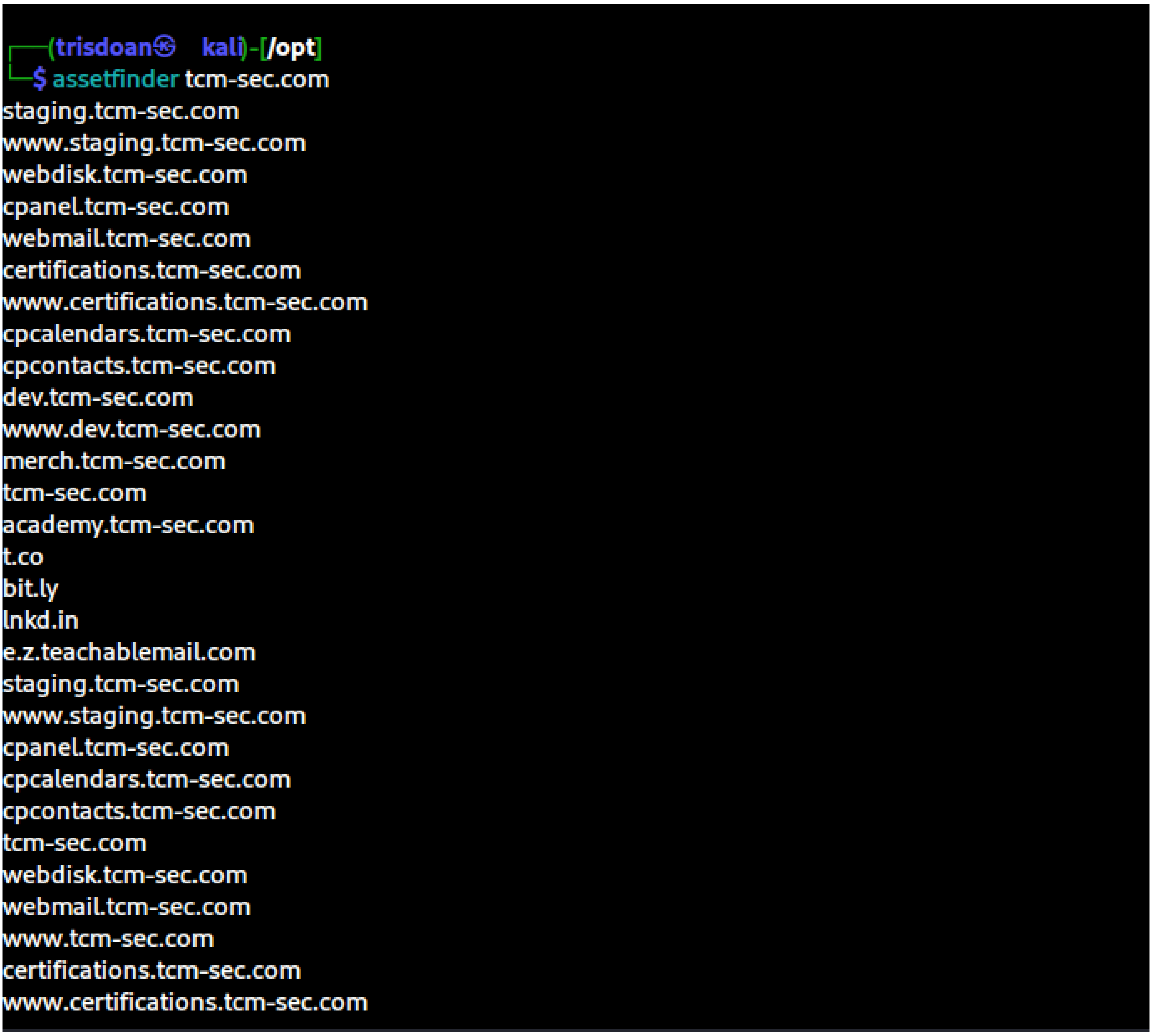
WHOIS

SUBFINDER (FIND SUBDOMAINS)



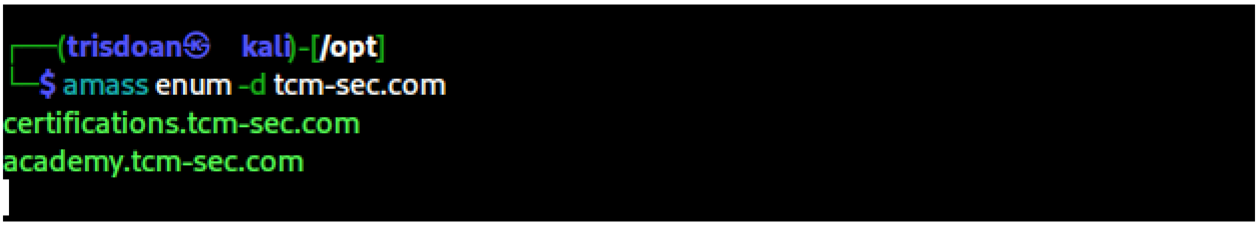
```
┌──(trisdoan㉿   kali)-[/opt]
└─$ subfinder -d tcm-sec.com


      _     __ _         _
____  _| |__ / _(_)_ _  __| |___ _ _
(_-< || | '_ \  _| | ' \/ _  / -_) '_|
/__/\_,_|_.__/_| |_|_||_\__,_\___|_| v2

          projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] By using s   finder, you also agree to the terms of the APIs used.

[INF] Enumerating subdomains for tcm-sec.com
www.tcm-sec.com
www.certifications.tcm-sec.com
webmail.tcm-sec.  om
webdisk.tcm-sec.  om
cpcontacts.tcm-sec.com
cpcalendars.tcm-sec.com
cpanel.tcm-sec.com
certifications.tcm-sec.com
academy.tcm-sec.com
mail.tcm-sec.com
merch.tcm-sec.com
www.staging.tcm-sec.com
staging.tcm-sec.com
www.academy.tcm-sec.com
dev.tcm-sec.com
www.dev.tcm-sec.com
```

ASSTERFINDER (FIND RELATIONS TO THAT DOMAINS)



```
┌──(trisdoan㉿ kali)-[/opt]
└─$ assetfinder tcm-sec.com
staging.tcm-sec.com
www.staging.tcm-sec.com
webdisk.tcm-sec.com
cpanel.tcm-sec.com
webmail.tcm-sec.com
certifications.tcm-sec.com
www.certifications.tcm-sec.com
cpcalendars.tcm-sec.com
cpcontacts.tcm-sec.com
dev.tcm-sec.com
www.dev.tcm-sec.com
merch.tcm-sec.com
tcm-sec.com
academy.tcm-sec.com
t.co
bit.ly
lnkd.in
e.z.teachablemail.com
staging.tcm-sec.com
www.staging.tcm-sec.com
cpanel.tcm-sec.com
cpcalendars.tcm-sec.com
cpcontacts.tcm-sec.com
tcm-sec.com
webdisk.tcm-sec.com
webmail.tcm-sec.com
www.tcm-sec.com
certifications.tcm-sec.com
www.certifications.tcm-sec.com
```

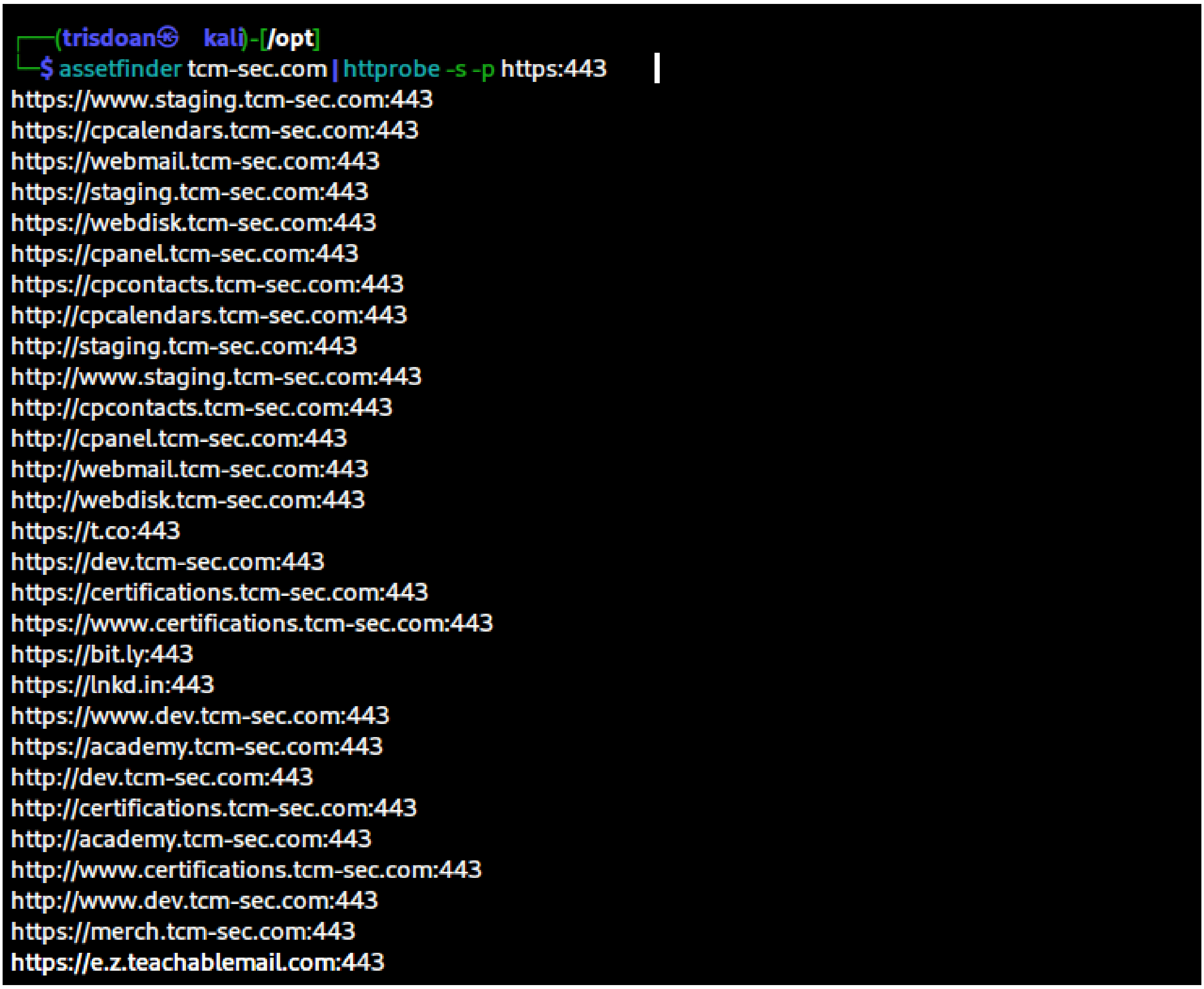
***AMASS (TRY TO LOOK FOR SUBDOMAINS). TAKE QUITE A TIME TO RUN CUZ IT IS BASED ON THE SIZE OF THE WEBSITE. ***



```
┌──(trisdoan㉿ kali)-[/opt]
└─$ amass enum -d tcm-sec.com
certifications.tcm-sec.com
academy.tcm-sec.com
```

***--

HTTPROBE (CHECK ALIVE DOMAINS)

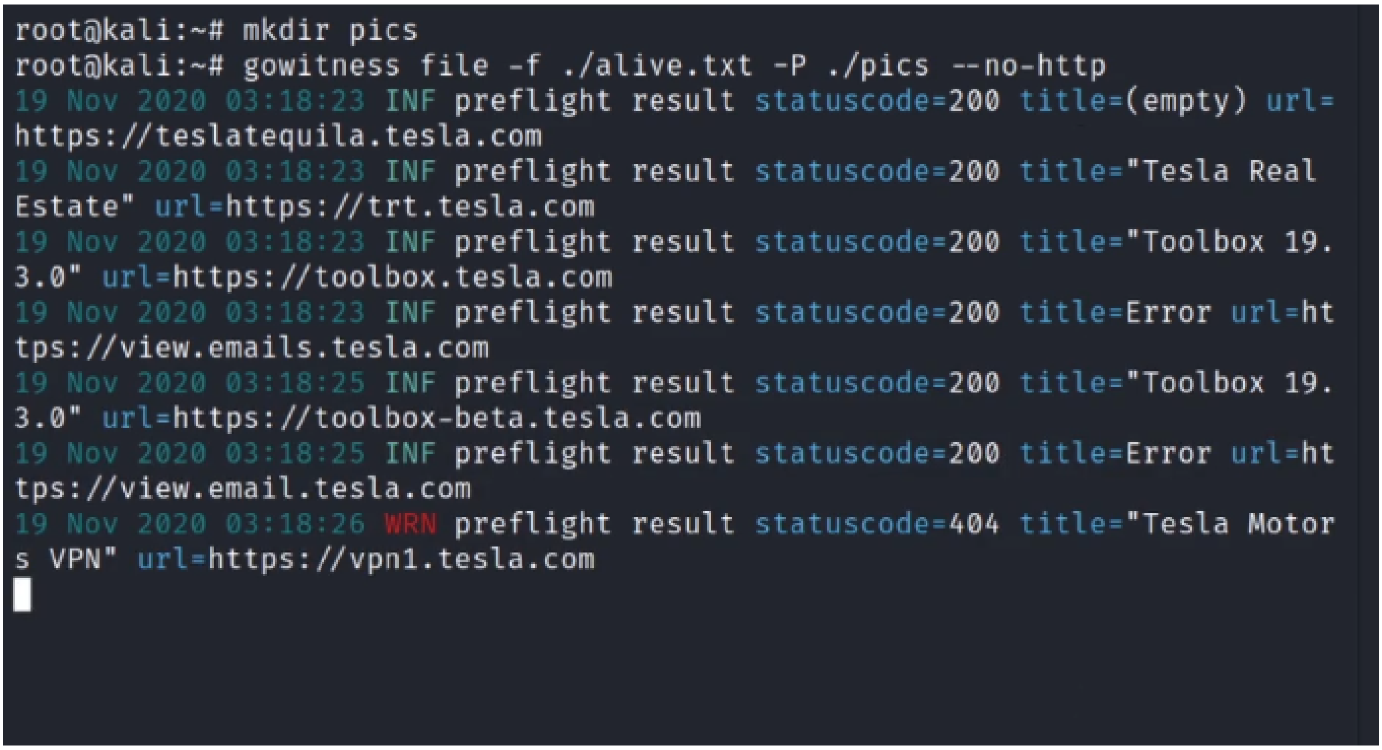


```
┌──(trisdoan㉿ kali)-[/opt]
└─$ assetfinder tcm-sec.com | httprobe -s -p https:443
https://www.staging.tcm-sec.com:443
https://cpcalendars.tcm-sec.com:443
https://webmail.tcm-sec.com:443
https://staging.tcm-sec.com:443
https://webdisk.tcm-sec.com:443
https://cpanel.tcm-sec.com:443
https://cpcontacts.tcm-sec.com:443
http://cpcalendars.tcm-sec.com:443
http://staging.tcm-sec.com:443
http://www.staging.tcm-sec.com:443
http://cpcontacts.tcm-sec.com:443
http://cpanel.tcm-sec.com:443
http://webmail.tcm-sec.com:443
http://webdisk.tcm-sec.com:443
https://t.co:443
https://dev.tcm-sec.com:443
https://certifications.tcm-sec.com:443
https://www.certifications.tcm-sec.com:443
https://bit.ly:443
https://lnkd.in:443
https://www.dev.tcm-sec.com:443
https://academy.tcm-sec.com:443
http://dev.tcm-sec.com:443
http://certifications.tcm-sec.com:443
http://academy.tcm-sec.com:443
http://www.certifications.tcm-sec.com:443
http://www.dev.tcm-sec.com:443
https://merch.tcm-sec.com:443
https://e.z.teachablemail.com:443
```

GOWITNESS (SCAN THRU EACH DOMAINS AND TAKE A SCREEN SHOT OF THAT WEBSITE)

-p: PATH

-F: FILE THAT CONTENT DOMAINS



```
root@kali:~# mkdir pics
root@kali:~# gowitness file -f ./alive.txt -P ./pics --no-http
19 Nov 2020 03:18:23 INF preflight result statuscode=200 title=(empty) url=
https://teslatequila.tesla.com
19 Nov 2020 03:18:23 INF preflight result statuscode=200 title="Tesla Real
Estate" url=https://trt.tesla.com
19 Nov 2020 03:18:23 INF preflight result statuscode=200 title="Toolbox 19.
3.0" url=https://toolbox.tesla.com
19 Nov 2020 03:18:23 INF preflight result statuscode=200 title=Error url=ht
tps://view.emails.tesla.com
19 Nov 2020 03:18:25 INF preflight result statuscode=200 title="Toolbox 19.
3.0" url=https://toolbox-beta.tesla.com
19 Nov 2020 03:18:25 INF preflight result statuscode=200 title=Error url=ht
tps://view.email.tesla.com
19 Nov 2020 03:18:26 WRN preflight result statuscode=404 title="Tesla Motor
s VPN" url=https://vpn1.tesla.com
```