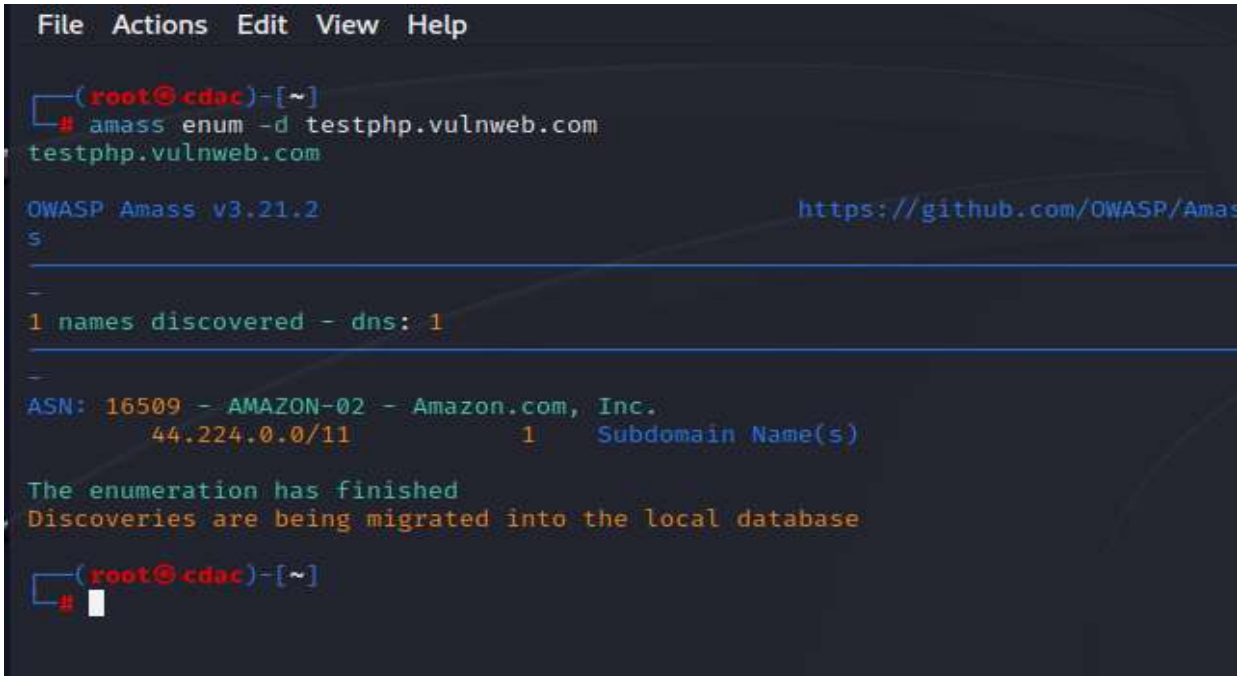
Lab: Information Gathering using AMASS Tool

a. **Basic Command to emun target**

amass enum -d testphp.vulnweb.com



b. **Mention Ports for the Scan**

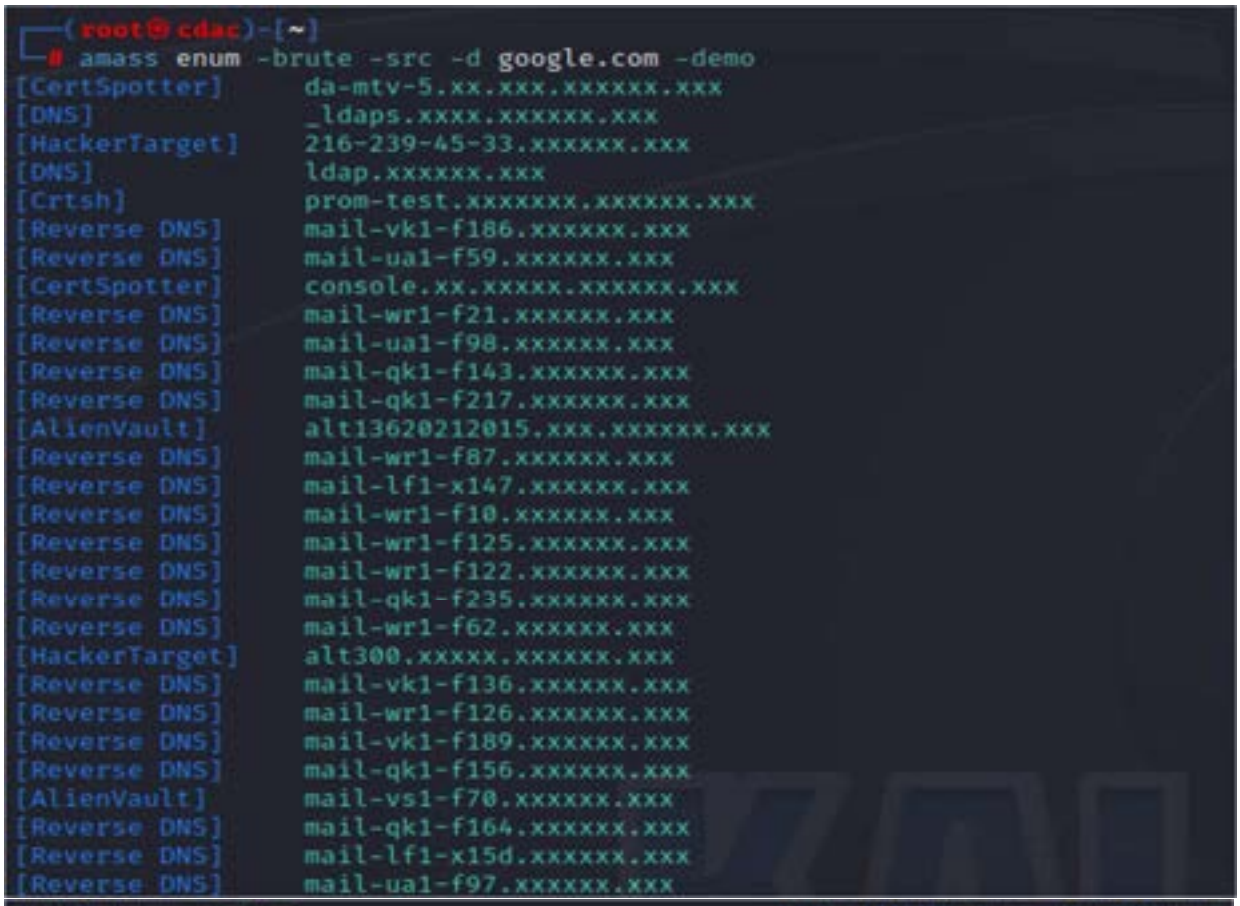
amass enum -d testphp.vulnweb.com 443, 8080

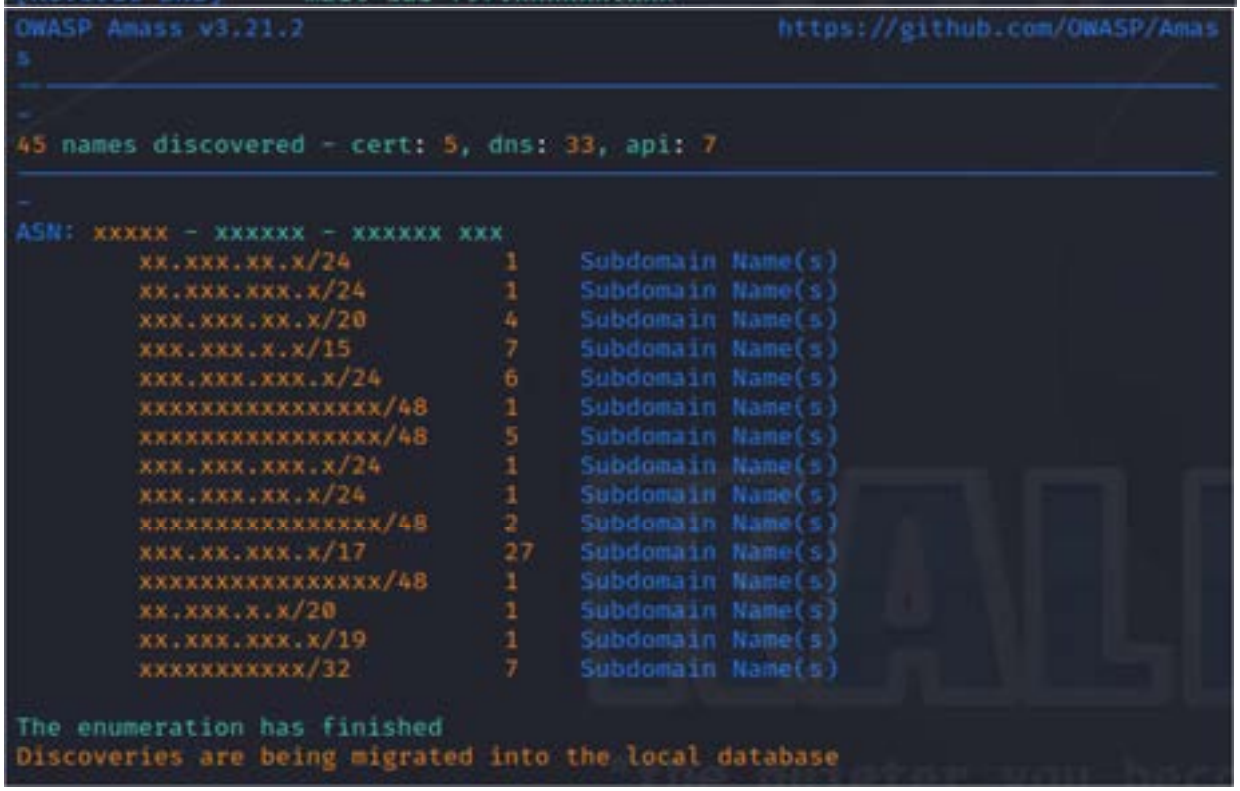
c. **Combining different options to get more refined results. -d options enable users to enter multiple URLs and -active options use active recon methods.**

amass enum -d testphp.vulnweb.com, google.com -active

d. Perform brute force by using - brute option for subdomain enumeration. -src option display data sources for the discovered names and -demo option display results in a presentable manner

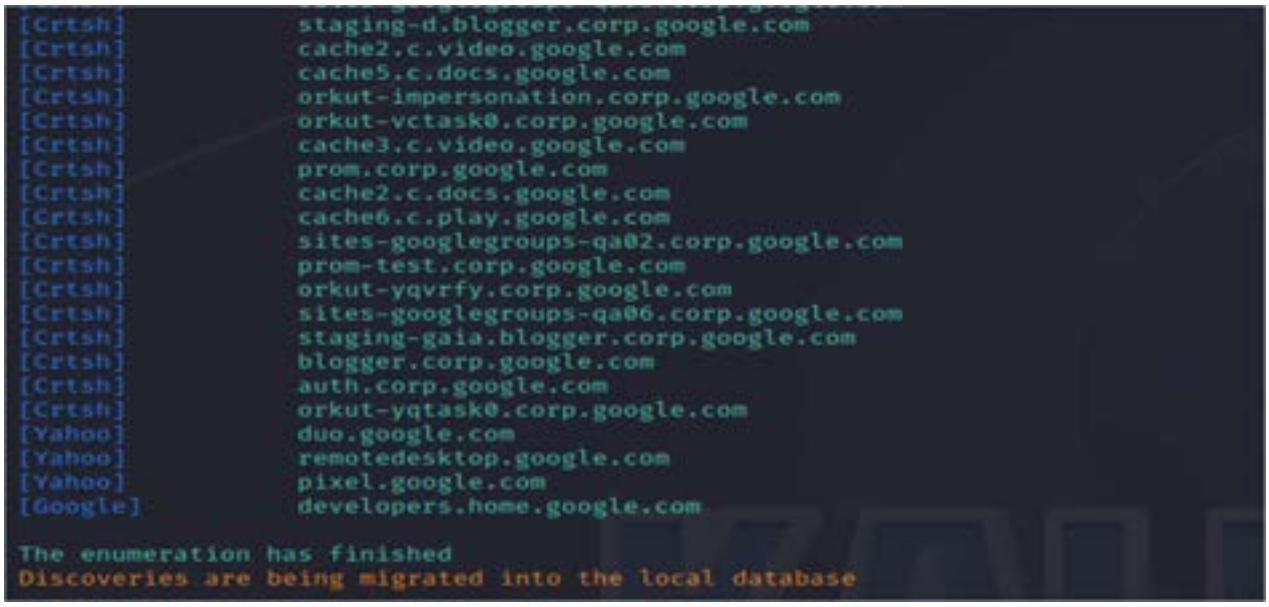
amass enum -brute -src -d google.com -demo





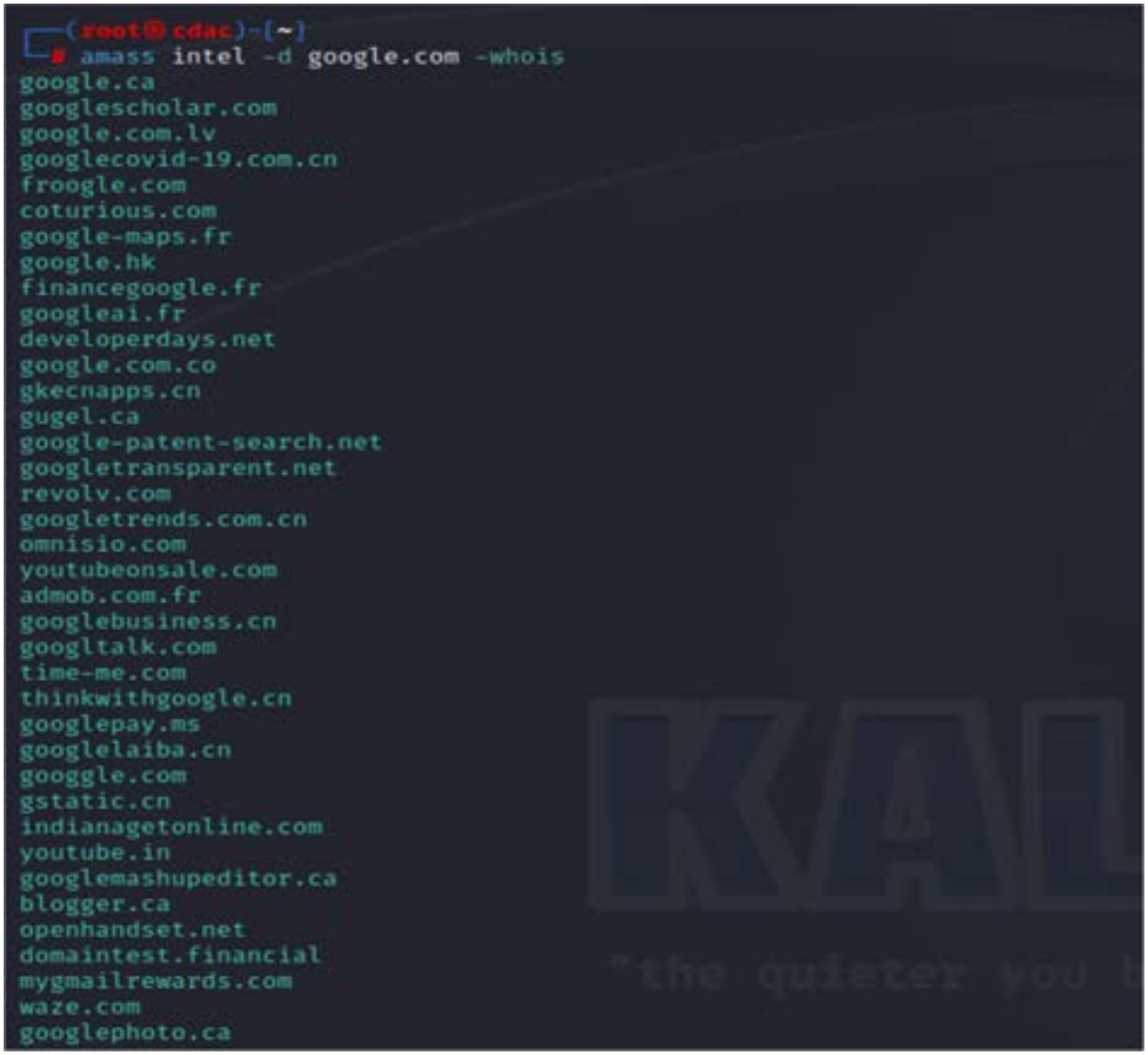
e. To do Passive Scanning

amass enum -passive -d google.com -src



f. Identify domains by using -whois option

amass intel -d google.com -whois



g. Enable active recon method

amass intel -active -cidr 172.31.0.0/15

h. Search Based on ASN

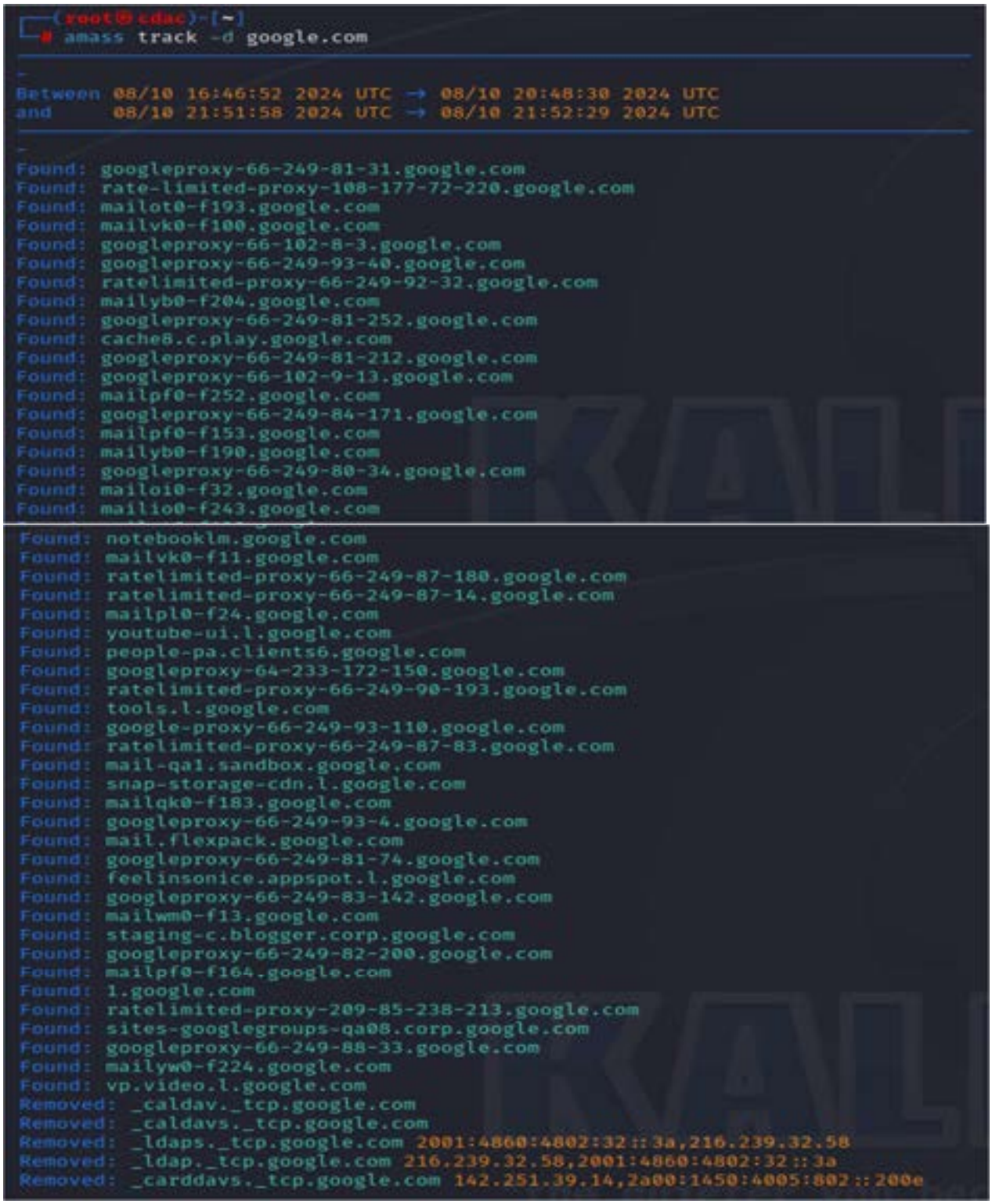
amass intel -asn 23314,81323

i. Search string based on AS description information

amass intel -org "google"

j. Basic command using track option

amass track -d google.com


┌──(root㉿cdac)-[~]
└─# amass track -d google.com
Between 08/10 16:46:52 2024 UTC → 08/10 20:48:30 2024 UTC
and 08/10 21:51:58 2024 UTC → 08/10 21:52:29 2024 UTC
Found: googleproxy-66-249-81-31.google.com
Found: rate-limited-proxy-108-177-72-220.google.com
Found: mailot0-f193.google.com
Found: mailvk0-f100.google.com
Found: googleproxy-66-102-8-3.google.com
Found: googleproxy-66-249-93-40.google.com
Found: ratelimited-proxy-66-249-92-32.google.com
Found: mailyb0-f204.google.com
Found: googleproxy-66-249-81-252.google.com
Found: cache8.c.play.google.com
Found: googleproxy-66-249-81-212.google.com
Found: googleproxy-66-102-9-13.google.com
Found: mailpf0-f252.google.com
Found: googleproxy-66-249-84-171.google.com
Found: mailpf0-f153.google.com
Found: mailyb0-f190.google.com
Found: googleproxy-66-249-80-34.google.com
Found: mailoi0-f32.google.com
Found: mailio0-f243.google.com

Found: notebooklm.google.com
Found: mailvk0-f11.google.com
Found: ratelimited-proxy-66-249-87-180.google.com
Found: ratelimited-proxy-66-249-87-14.google.com
Found: mailpl0-f24.google.com
Found: youtube-ui.l.google.com
Found: people-pa.clients6.google.com
Found: googleproxy-64-233-172-150.google.com
Found: ratelimited-proxy-66-249-90-193.google.com
Found: tools.l.google.com
Found: google-proxy-66-249-93-110.google.com
Found: ratelimited-proxy-66-249-87-83.google.com
Found: mail-qa1.sandbox.google.com
Found: snap-storage-cdn.l.google.com
Found: mailqk0-f183.google.com
Found: googleproxy-66-249-93-4.google.com
Found: mail.flexpack.google.com
Found: googleproxy-66-249-81-74.google.com
Found: feelinsonice.appspot.l.google.com
Found: googleproxy-66-249-83-142.google.com
Found: mailwm0-f13.google.com
Found: staging-c.blogger.corp.google.com
Found: googleproxy-66-249-82-200.google.com
Found: mailpf0-f164.google.com
Found: 1.google.com
Found: ratelimited-proxy-209-85-238-213.google.com
Found: sites-googlegroups-qa08.corp.google.com
Found: googleproxy-66-249-88-33.google.com
Found: mailyw0-f224.google.com
Found: vp.video.l.google.com
Removed: _caldav._tcp.google.com
Removed: _caldavs._tcp.google.com
Removed: _ldaps._tcp.google.com 2001:4860:4802:32::3a,216.239.32.58
Removed: _ldap._tcp.google.com 216.239.32.58,2001:4860:4802:32::3a
Removed: _carddavs._tcp.google.com 142.251.39.14,2a00:1450:4005:802::200e