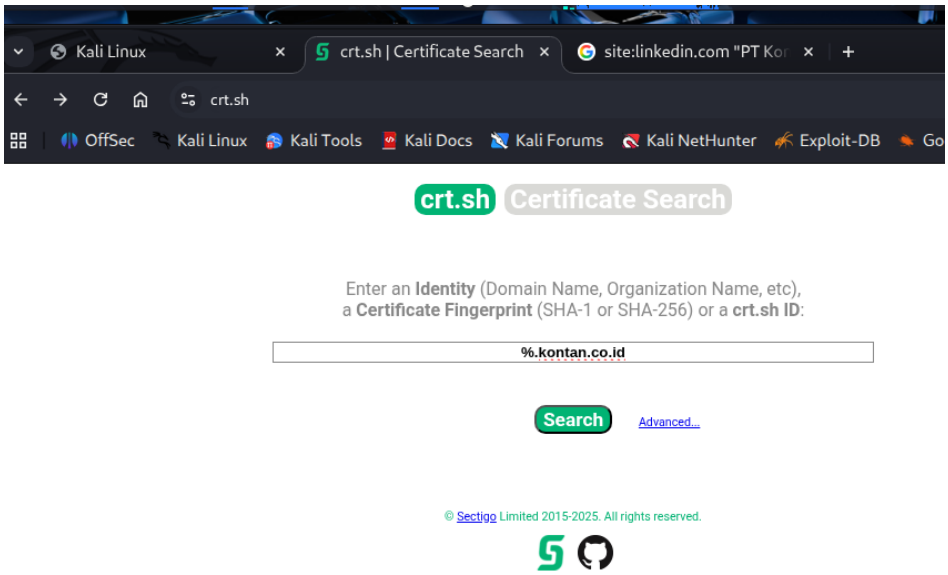
SKENARIO

1. Passive Reconnaissance (Pengintaian Pasif)
   a. Pencarian Domain dan Sub-domain
      - Masuk terlebih di vm kalinux dan jalankan
      - Masuk di terminal kemudian ketikkan sesui gambar di bawah
      - Domain WHOIS dan Infrastruktur

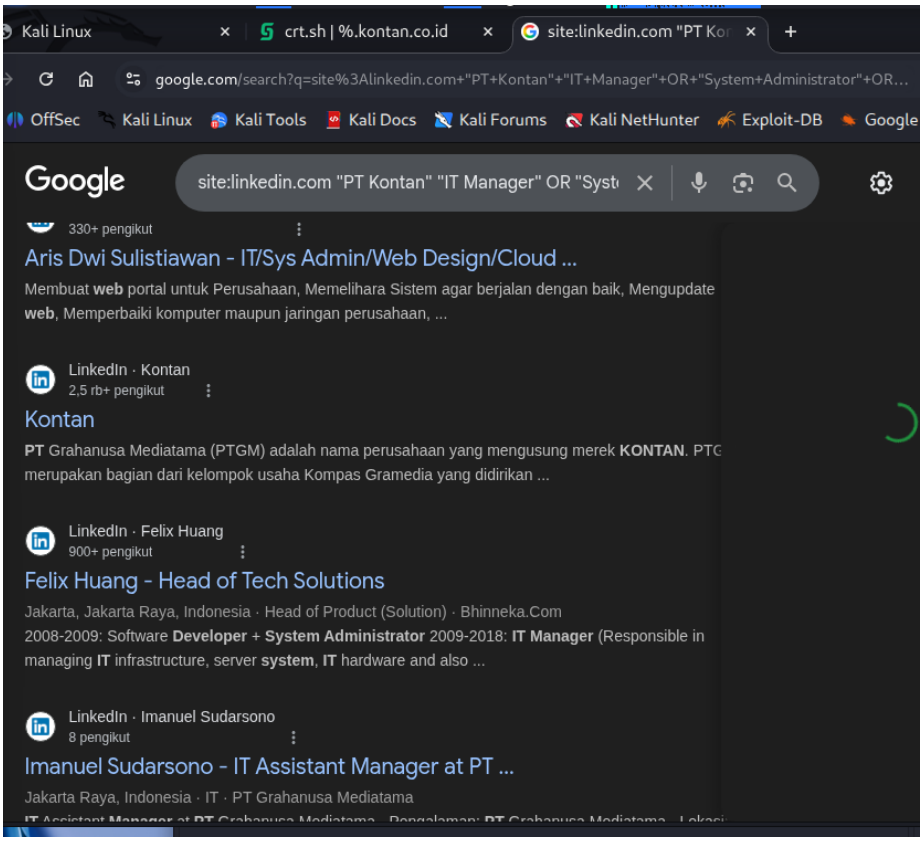
memulai dengan perintah whois kontan.co.id untuk mengetahui detail pendaftaran domain. Hasilnya mengidentifikasi *Nameserver* utama (NS1.DNS-PARKING.COM) dan *Registrar*. Informasi ini penting untuk memahami di mana DNS target dikelola.

Ketikkan perintah https://crt.sh lalu masukkan di kolom %.kontan.co.id sampai hasilnya muncul seperti di gambar bawah



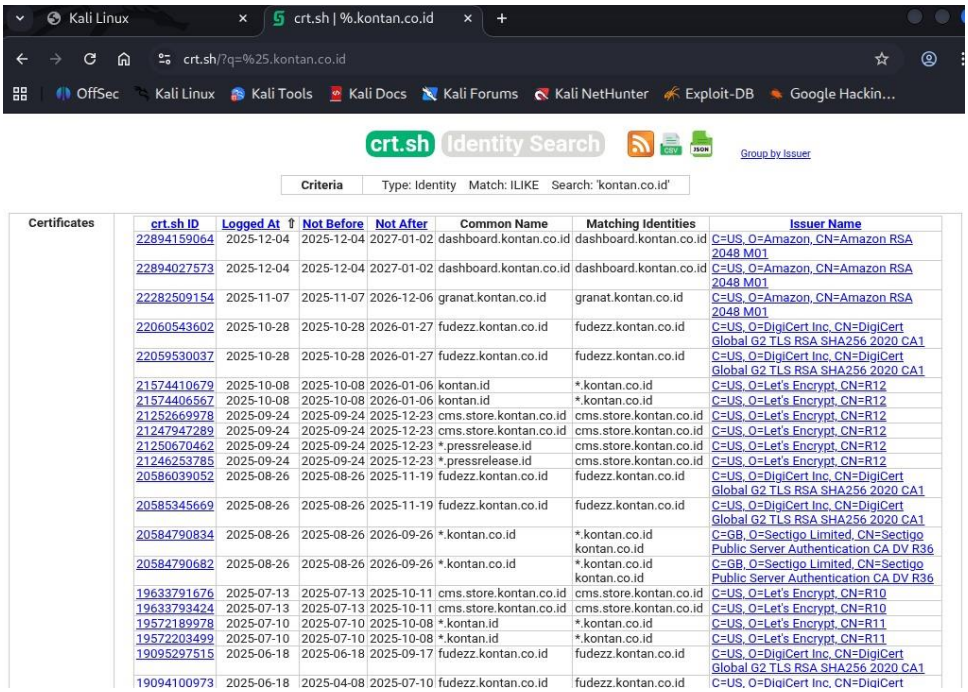
b. Informasi Email dan Karyawan

- mengumpulkan informasi tentang karyawan dan struktur internal target dengan inputan site:linkedin.com "PT Kontan" "IT Manager" OR "System Administrator" OR "Web Developer" di browser kali linux



Dari hasil pencarian, muncul profil LinkedIn milik **Aris Dwi Sulistiawan, Felix Huang,** dan **Imanuel sudarsono**

- pola email resmi PT Kontan untuk menentukan format email perusahaan



crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
22894159064	2025-12-04	2025-12-04	2027-01-02	dashboard.kontan.co.id	dashboard.kontan.co.id	C=US, O=Amazon, CN=Amazon RSA 2048 M01
22894027573	2025-12-04	2025-12-04	2027-01-02	dashboard.kontan.co.id	dashboard.kontan.co.id	C=US, O=Amazon, CN=Amazon RSA 2048 M01
22282509154	2025-11-07	2025-11-07	2026-12-06	granat.kontan.co.id	granat.kontan.co.id	C=US, O=Amazon, CN=Amazon RSA 2048 M01
22060543602	2025-10-28	2025-10-28	2026-01-27	fudezz.kontan.co.id	fudezz.kontan.co.id	C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
22059530037	2025-10-28	2025-10-28	2026-01-27	fudezz.kontan.co.id	fudezz.kontan.co.id	C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
21574410679	2025-10-08	2025-10-08	2026-01-06	kontan.id	*.kontan.co.id	C=US, O=Let's Encrypt, CN=R12
21574406567	2025-10-08	2025-10-08	2026-01-06	kontan.id	*.kontan.co.id	C=US, O=Let's Encrypt, CN=R12
21252669978	2025-09-24	2025-09-24	2025-12-23	cms.store.kontan.co.id	cms.store.kontan.co.id	C=US, O=Let's Encrypt, CN=R12
21247947289	2025-09-24	2025-09-24	2025-12-23	cms.store.kontan.co.id	cms.store.kontan.co.id	C=US, O=Let's Encrypt, CN=R12
21250670462	2025-09-24	2025-09-24	2025-12-23	*.pressrelease.id	cms.store.kontan.co.id	C=US, O=Let's Encrypt, CN=R12
21246253785	2025-09-24	2025-09-24	2025-12-23	*.pressrelease.id	cms.store.kontan.co.id	C=US, O=Let's Encrypt, CN=R12
20586039052	2025-08-26	2025-08-26	2025-11-19	fudezz.kontan.co.id	fudezz.kontan.co.id	C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
20585345669	2025-08-26	2025-08-26	2025-11-19	fudezz.kontan.co.id	fudezz.kontan.co.id	C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
20584790834	2025-08-26	2025-08-26	2026-09-26	*.kontan.co.id	*.kontan.co.id kontan.co.id	C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV R36
20584790682	2025-08-26	2025-08-26	2026-09-26	*.kontan.co.id	*.kontan.co.id kontan.co.id	C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV R36
19633791676	2025-07-13	2025-07-13	2025-10-11	cms.store.kontan.co.id	cms.store.kontan.co.id	C=US, O=Let's Encrypt, CN=R10
19633793424	2025-07-13	2025-07-13	2025-10-11	cms.store.kontan.co.id	cms.store.kontan.co.id	C=US, O=Let's Encrypt, CN=R10
19572189978	2025-07-10	2025-07-10	2025-10-08	*.kontan.id	*.kontan.co.id	C=US, O=Let's Encrypt, CN=R11
19572203499	2025-07-10	2025-07-10	2025-10-08	*.kontan.id	*.kontan.co.id	C=US, O=Let's Encrypt, CN=R11
19095297515	2025-06-18	2025-06-18	2025-09-17	fudezz.kontan.co.id	fudezz.kontan.co.id	C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
19094100973	2025-06-18	2025-04-08	2025-07-10	fudezz.kontan.co.id	fudezz.kontan.co.id	C=US, O=DigiCert Inc, CN=DigiCert

terlihat beberapa alamat email aktif, yaitu:

- redaksi@kontan.co.id
- kontannews@kontan.co.id

Ini menunjukkan bahwa Kontan menggunakan role-based email yang berbasis fungsi divisi, bukan email berbasis nama pribadi.

Bukti Keberhasilan OSINT:

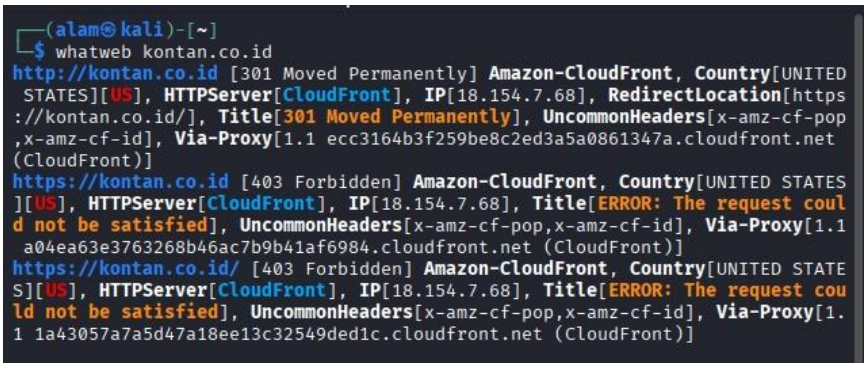
Gambar ini membuktikan bahwa teknik OSINT berhasil menemukan format email nyata yang digunakan oleh PT Kontan.

Dengan bukti ini, kamu dapat menyimpulkan format email lain yang mungkin digunakan untuk divisi teknis, seperti:

- it@kontan.co.id
- support@kontan.co.id
- admin@kontan.co.id

c. Teknologi yang Digunakan

- Teknologi Utama



Perintah whatweb kontan.co.id digunakan untuk melihat teknologi yang dipakai situs. Hasilnya menunjukkan bahwa website menggunakan Amazon CloudFront (CDN) sehingga tidak terlihat adanya file konfigurasi, backup, atau kredensial yang bocor. Hal ini berarti tidak ada informasi sensitif yang terpapar pada lapisan depan situs. WhatWeb hanya dapat melihat teknologi permukaan karena CDN menyembunyikan server asli.Active Reconnaissance (Pengintaian Aktif)

- Informasi Sensitif yang Terpapar

  Pemeriksaan dilakukan menggunakan Google Dorks, GitHub search, dan Pastebin search. Berdasarkan pencarian tersebut tidak ditemukan informasi sensitif yang terpapar, seperti file konfigurasi, kredensial, atau backup. Tidak adanya temuan juga didukung oleh hasil WhatWeb, yang menunjukkan situs menggunakan Amazon CloudFront, sehingga lapisan depan situs terlindungi dan tidak menampilkan file sensitif.

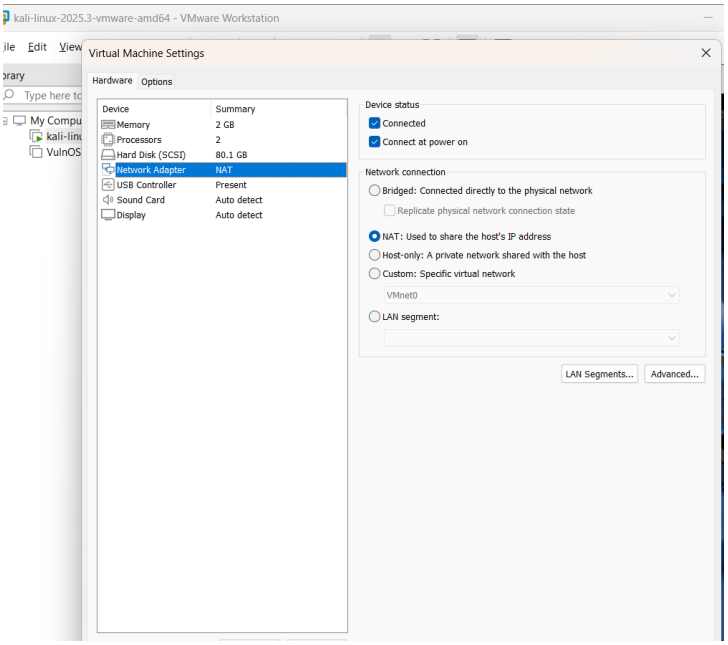
2. **Active Reconnaissance (Pengintaian Aktif)**

   Active Recon adalah tahap pengumpulan informasi yang melibatkan interaksi langsung dengan sistem target.

   hasil active reconnaissance

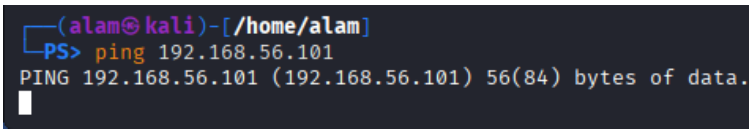
   a. Host Discovery dan Port Scanning

- Pastikan host only di kali linux



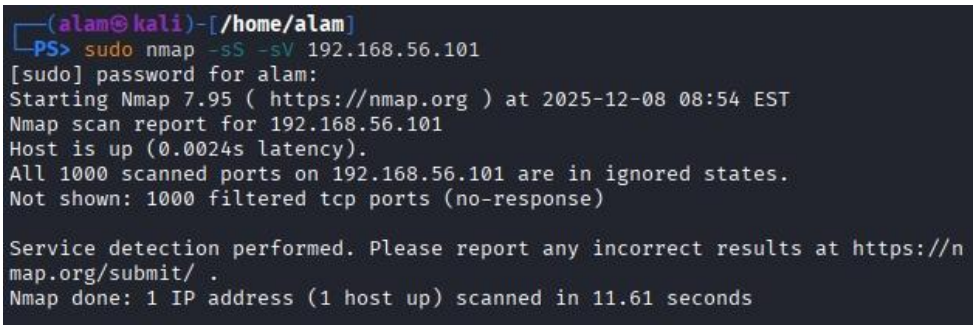
Bukti konfigurasi jaringan VM Host-only yang digunakan untuk lingkungan lab.

- *Host Discovery* berhasil



Bukti awal *Host Discovery* berhasil (target hidup) sebelum pemblokiran penuh.

- Pemindaian Port & Versi (Active Recon)



Bukti kegagalan Nmap SYN Scan (-sS), yang menunjukkan *firewall* ketat memblokir semua port.Active Reconnaissance dilakukan terhadap target lab 192.168.56.101.

- kegagalan Nmap TCP Connect Scan

```
┌──(alam㉿kali)-[/home/alam]
└─PS> sudo nmap -sT -sV -O -Pn 192.168.56.101
[sudo] password for alam:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 09:07 EST
Nmap scan report for 192.168.56.101
Host is up (0.00064s latency).
All 1000 scanned ports on 192.168.56.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: D-Link DFL-700 firewall (89%), HP Officejet Pro 8500 p
rinter (89%), IBM i 7.4 (89%), ReactOS 0.3.7 (89%), Sanyo PLC-XU88 digital vi
deo projector (89%), Sonus GSX9000 VoIP proxy (88%), Asus WL-500gP wireless b
roadband router (88%), Microsoft Windows 2000 (88%), Microsoft Windows Server
 2003 Enterprise Edition SP2 (88%), Microsoft Windows Server 2003 SP2 (88%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 209.61 seconds
```

Bukti kegagalan Nmap TCP Connect Scan (-sT), yang digunakan sebagai dasar asumsi layanan rentan.

- hasil UDP Scan (-sU)

```
┌──(alam㉿kali)-[~]
└─$ sudo nmap -sU -Pn -vv 192.168.56.101
[sudo] password for alam:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 14:14 EST
Initiating Parallel DNS resolution of 1 host. at 14:14
Completed Parallel DNS resolution of 1 host. at 14:14, 0.03s elapsed
Initiating UDP Scan at 14:14
Scanning 192.168.56.101 [1000 ports]
UDP Scan Timing: About 13.55% done; ETC: 14:18 (0:03:18 remaining)
UDP Scan Timing: About 28.05% done; ETC: 14:17 (0:02:36 remaining)
UDP Scan Timing: About 43.05% done; ETC: 14:17 (0:02:00 remaining)
UDP Scan Timing: About 57.55% done; ETC: 14:17 (0:01:29 remaining)
UDP Scan Timing: About 72.50% done; ETC: 14:17 (0:00:57 remaining)
Completed UDP Scan at 14:17, 208.80s elapsed (1000 total ports)
Nmap scan report for 192.168.56.101
Host is up, received user-set.
Scanned at 2025-12-08 14:14:17 EST for 207s
All 1000 scanned ports on 192.168.56.101 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 209.08 seconds
           Raw packets sent: 2090 (98.700KB) | Rcvd: 1 (112B)
```

Perintah sudo nmap -sU -Pn -vv 192.168.56.101 digunakan untuk memindai seluruh port UDP pada target. Hasil menunjukkan bahwa host terdeteksi hidup, namun semua 1000 port UDP berada pada status open/filtered (no response). Ini berarti target tidak memberikan respons apa pun terhadap paket UDP, sehingga Nmap tidak dapat memastikan apakah port tersebut terbuka atau diblokir oleh firewall. Kondisi ini menandakan adanya filtering ketat pada lalu lintas UDP.

b. Service and Version Detection

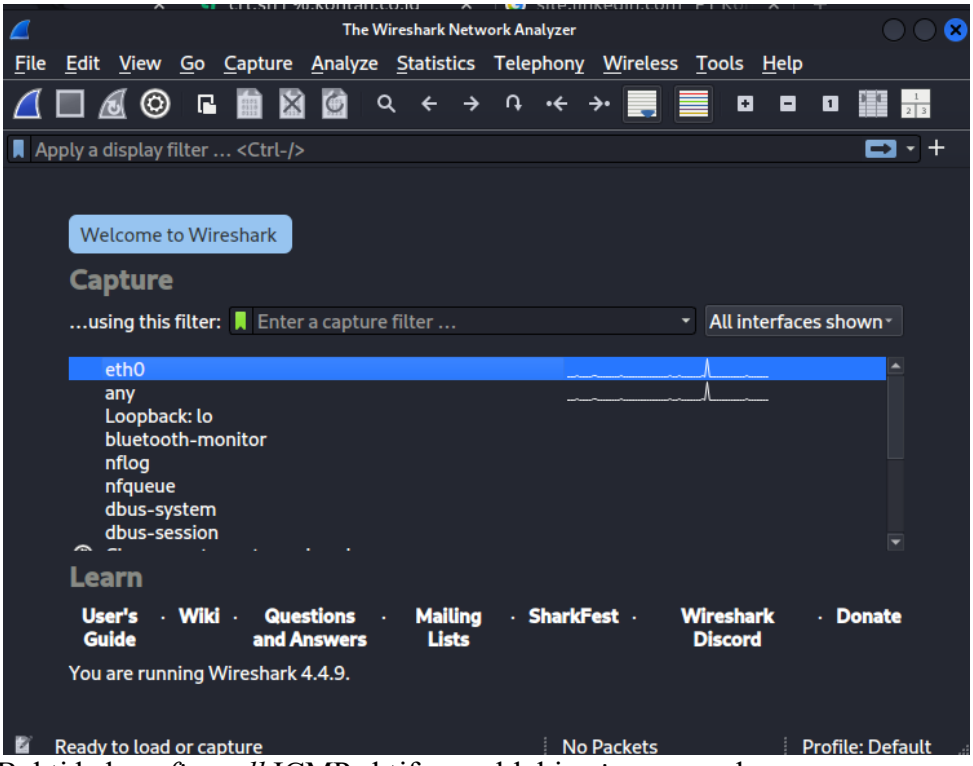
Tahap ini tidak dapat dilakukan karena seluruh port TCP dan UDP pada target berada dalam keadaan *filtered* atau tidak merespons. Firewall menolak semua koneksi sehingga tidak ada port terbuka yang bisa dianalisis untuk mengetahui layanan maupun versi software.

c. OS Fingerprinting

OS fingerprinting gagal karena semua jenis probe yang dikirim (ICMP, SYN, TCP Connect, dan UDP) diblokir firewall. Tidak ada respons balik yang dapat digunakan Nmap untuk menebak sistem operasi target.

d. Network Protocol Analysis

- *firewall* ICMP aktif



Bukti bahwa *firewall* ICMP aktif, memblokir *ping* sepenuhnya.

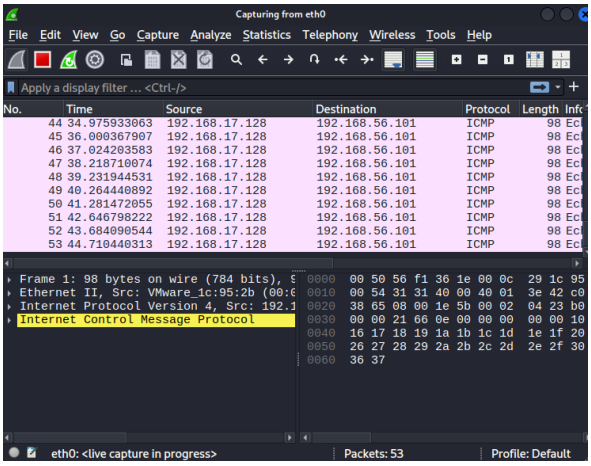
- Masuk di wireshark pilih eth0 dan klik sirip biru untuk memulai

```
┌──(alam㉿kali)-[/home/alam]
└─PS> ping -c 5 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.

── 192.168.56.101 ping statistics ──
5 packets transmitted, 0 received, 100% packet loss, time 4098ms
```

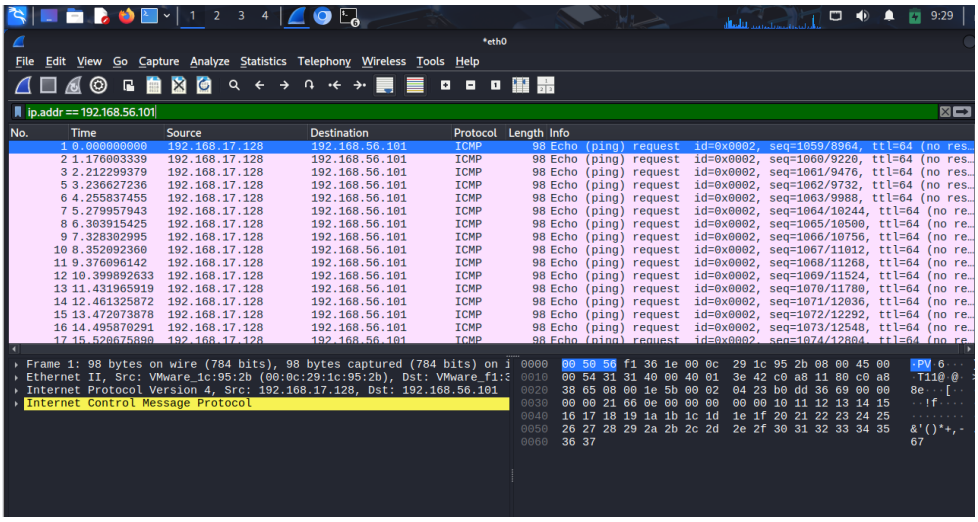
Bukti persiapan alat Wireshark untuk Analisis Protokol.

- Analisis Protokol



Pencet kotak merah unutk mengentikan

- Analisis Protokol dengan mengetik ip.addr = 192.168.56.101



digunakan untuk menampilkan hanya paket jaringan yang berasal atau menuju IP 192.168.56.101 agar analisis Wireshark lebih fokus dan tidak bercampur

dengan trafik lain. Bukti hasil Analisis Protokol, berhasil menangkap paket ICMP yang dikirim.