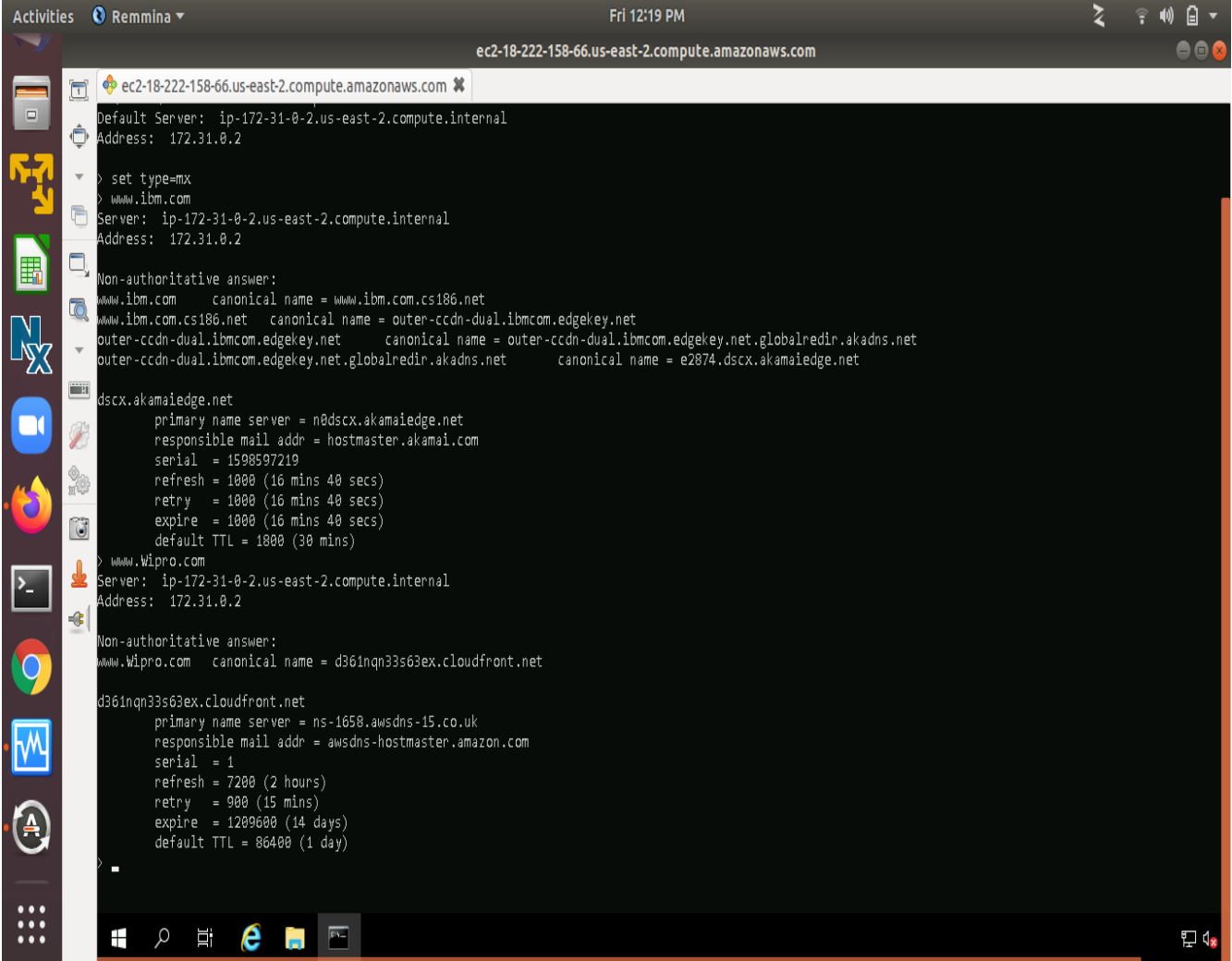


1)



The screenshot shows a Remmina terminal window titled "ec2-18-222-158-66.us-east-2.compute.amazonaws.com". The terminal displays the output of a series of DNS lookups. It starts with a "Default Server" and "Address" for ip-172-31-0-2.us-east-2.compute.internal. Then, it shows the results of a "set type=mx" command for www.ibm.com, followed by a series of canonical name lookups for the IBM domain chain. Next, it shows the results of a lookup for dscx.akamaiedge.net, including its primary name server and refresh/retry/expire times. Finally, it shows the results of a lookup for www.wipro.com, including its canonical name and primary name server details.

```
ec2-18-222-158-66.us-east-2.compute.amazonaws.com X
Default Server: ip-172-31-0-2.us-east-2.compute.internal
Address: 172.31.0.2

> set type=mx
> www.ibm.com
Server: ip-172-31-0-2.us-east-2.compute.internal
Address: 172.31.0.2

Non-authoritative answer:
www.ibm.com canonical name = www.ibm.com.cs186.net
www.ibm.com.cs186.net canonical name = outer-ccdn-dual.ibmcom.edgekey.net
outer-ccdn-dual.ibmcom.edgekey.net canonical name = outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net
outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net canonical name = e2874.dscx.akamaiedge.net

dscx.akamaiedge.net
primary name server = n0dscx.akamaiedge.net
responsible mail addr = hostmaster.akamai.com
serial = 1598597219
refresh = 1000 (16 mins 40 secs)
retry = 1000 (16 mins 40 secs)
expire = 1000 (16 mins 40 secs)
default TTL = 1800 (30 mins)

> www.wipro.com
Server: ip-172-31-0-2.us-east-2.compute.internal
Address: 172.31.0.2

Non-authoritative answer:
www.wipro.com canonical name = d361qn33s63ex.cloudfront.net

d361qn33s63ex.cloudfront.net
primary name server = ns-1658.awsdns-15.co.uk
responsible mail addr = awsdns-hostmaster.amazon.com
serial = 1
refresh = 7200 (2 hours)
retry = 900 (15 mins)
expire = 1209600 (14 days)
default TTL = 86400 (1 day)
```

eMailTrackerPro v10.0b Advanced Edition. Trial day 1 of 15

File Help

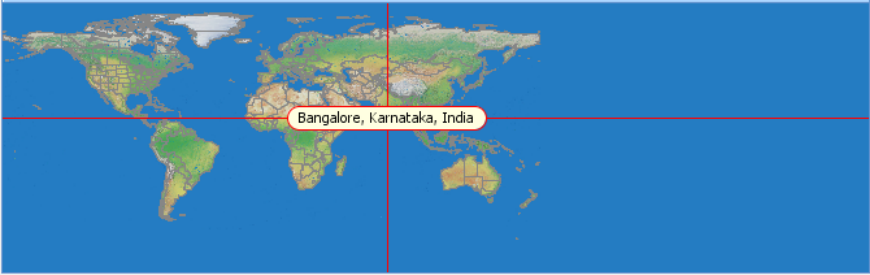
My Inbox My Trace Reports Trace Headers Trace Address Email Accounts Settings Export Rules Trial Edition

View New Email Trace Configure

Home Subject: Invitation to... Subject: careers at wipro X

The trace is complete, the information found is displayed on the right [New Trace](#) [View Report](#)

Map



Bangalore, Karnataka, India

Table #	Hop IP	Hop Name	Location
1	10.0.2.2		
2	192.168.43.1	_gateway	
4	10.72.0.83		
5	172.25.75.91		
6	172.25.75.86		
7	172.25.9.165		
13	49.44.129.54		(Australia)
15	125.21.179.222		(India)
End	203.91.199.24		Bangalore, Karnataka, India

Email Summary

From: careers@wipro.com
 To: ravadaravikiran300@gmail.com
 Date: Mon, 17 Jun 2019 05:00:47 +0530
 Subject: careers at wipro
 Location: Bangalore, Karnataka, India

Misdirected: Yes (Possibly spam)
Abuse Address: abuse-ip@wipro.com
Abuse Reporting: To automatically generate an email abuse report [click here](#)
From IP: 203.91.199.24

Header Analysis:
 This email contains misdirection (The sender has attempted to hide their IP). The sender claimed to have name wipro-blr-tls01.wipro.com but a lookup on that name shows it couldn't have originated from sender IP - 203.91.199.24

System Information:

[Network Whois](#)

[Domain Whois](#)

[Email Header](#)

For 24 hours only you can get up to 20% off eMailTrackerPro! [Click Here](#)

Windows taskbar: Type here to search, e, 2:16 PM, 8/28/2020

2)

eMailTrackerPro v10.0b Advanced Edition. Trial day 1 of 15

File Help

My Inbox My Trace Reports Trace Headers Trace Address Email Accounts Settings Export Rules Trial Edition

View New Email Trace Configure

Home Subject: Invitation to... X

The trace is complete, the information found is displayed on the right

New Trace View Report

Email Summary

From: contest@techgig.com
 To: ravadaravikiran300@gmail.com
 Date: 22 Jun 2020 08:11:36 +0530
 Subject: Invitation to participate in Code Gladiators >meta h
 Location: Pune, Maharashtra, India

Misdirected: No
 Abuse Address: 4755abuse@tatacommunications.com
 Abuse Reporting: To automatically generate an email abuse
 From IP: 219.65.84.187

System Information:

- There is no SMTP server running on this system (the p
- There is no HTTP server running on this system (the p
- There is no HTTPS server running on this system (the p
- There is no FTP server running on this system (the po

Table #	Hop IP	Hop Name	Location
1	10.0.2.2		
2	192.168.43.1	_gateway	
4	10.72.0.35		
5	172.25.75.87		
6	172.25.75.86		
7	172.25.9.165		
13	115.112.8.117	115.112.8.117.STATIC-Chennai.v	(India)
15	14.142.155.186	14.142.155.186.static-Mumbai.v	Mumbai, India
16	103.18.140.92		India

For 24 hours only you can get up to 20% off eMailTrackerPro! [Click Here](#)

Invitation to participate in C Original Message eMailTrackerPro Report

file:///C:/Users/ravikiran/eMailTrackerPro/V8/reports/report-20200828-1420-2.html

descr: Data and Voice Carrier in India
admin-c: TC651-AP
tech-c: TC651-AP
country: IN
org: ORG-TCL6-AP
remarks: -+-+-+
-+-+-+
remarks: This object can only be modified by APNIC
hostmaster
remarks: If you wish to modify this object details
please
remarks: send email to hostmaster@apnic.net with
your organisation
remarks: account name in the subject line.
remarks: -+-+-+
-+-+-+
mnt-by: APNIC-HM
mnt-lower: MAINT-TATACOMM-IN
mnt-routes: MAINT-TATACOMM-IN
mnt-irt: IRT-TATACOMM-IN
status: ALLOCATED PORTABLE
last-modified: 2017-08-30T07:19:50Z
source: APNIC

irt: IRT-TATACOMM-IN
address: 6th Floor, LVSB, VSNL
address: Kashinath Dhuru marg, Prabhadevi
address: Dadar(W), Mumbai 400028
address: India
e-mail: ip.admin@tatacommunications.com
abuse-mailbox: 4755abuse@tatacommunications.com
admin-c: IA15-AP
tech-c: IA15-AP
auth: # Filtered
remarks: ip.admin@tatacommunications.com is invalid
remarks: 4755abuse@tatacommunications.com is
invalid
mnt-by: MAINT-TATACOMM-IN
last-modified: 2019-11-27T13:56:13Z
source: APNIC

Type here to search

ENG 2:22 PM
IN 8/28/2020


```
Applications  Places  Terminal  Aug 28 14:57  1  kali@kali: ~  
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~/... x  
root@kali:/home/kali# nmap -Pn -sS 192.168.43.168  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 14:56 EDT  
Nmap scan report for ravikiran-ThinkPad-L470 (192.168.43.168)  
Host is up (0.00080s latency).  
Not shown: 994 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
445/tcp    open  microsoft-ds  
631/tcp    open  ipp  
902/tcp    open  iss-realsure  
7070/tcp   open  realserver  
8080/tcp   open  http-proxy  
  
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds  
root@kali:/home/kali#
```

3)

```
Applications  Places  Terminal  Aug 28 14:58  1  [system icons]
kali@kali: ~
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~/... x
root@kali:/home/kali# nmap -Pn -sS -A -v 192.168.43.168
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 14:49 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:49
Completed NSE at 14:49, 0.00s elapsed
Initiating NSE at 14:49
Completed NSE at 14:49, 0.00s elapsed
Initiating NSE at 14:49
Completed NSE at 14:49, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 14:49
Completed Parallel DNS resolution of 1 host. at 14:49, 0.00s elapsed
Initiating SYN Stealth Scan at 14:49
Scanning ravikiran-ThinkPad-L470 (192.168.43.168) [1000 ports]
Discovered open port 22/tcp on 192.168.43.168
Discovered open port 445/tcp on 192.168.43.168
Discovered open port 8080/tcp on 192.168.43.168
Discovered open port 7070/tcp on 192.168.43.168
Discovered open port 902/tcp on 192.168.43.168
Discovered open port 631/tcp on 192.168.43.168
Completed SYN Stealth Scan at 14:49, 0.28s elapsed (1000 total ports)
Initiating Service scan at 14:49
Scanning 6 services on ravikiran-ThinkPad-L470 (192.168.43.168)
Completed Service scan at 14:49, 19.07s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against ravikiran-ThinkPad-L470 (192.168.43.168)
Retrying OS detection (try #2) against ravikiran-ThinkPad-L470 (192.168.43.168)
Retrying OS detection (try #3) against ravikiran-ThinkPad-L470 (192.168.43.168)
Retrying OS detection (try #4) against ravikiran-ThinkPad-L470 (192.168.43.168)
Retrying OS detection (try #5) against ravikiran-ThinkPad-L470 (192.168.43.168)
Initiating Traceroute at 14:49
Completed Traceroute at 14:49, 0.01s elapsed
```



```
Applications Places Terminal Aug 28 14:58
kali@kali: ~
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~/... x
Nmap scan report for ravikiran-ThinkPad-L470 (192.168.43.168)
Host is up (0.00043s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b8:be:f9:f4:c4:b5:d0:2d:47:45:c1:4b:4e:c5:3c:51 (RSA)
|   256 02:54:dd:29:de:ff:55:78:ea:03:2d:df:f9:60:88:15 (ECDSA)
|_  256 f5:09:a4:5a:20:28:fd:08:b4:a8:88:fe:33:f6:85:d0 (ED25519)
445/tcp   open  netbios-ssn  Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
631/tcp   open  ipp          CUPS 2.2
|_ http-methods:
|   Supported Methods: GET HEAD OPTIONS POST PUT
|_ Potentially risky methods: PUT
|_ http-robots.txt: 1 disallowed entry
|_/
|_ http-server-header: CUPS/2.2 IPP/2.1
|_ http-title: Home - CUPS 2.2.7
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
7070/tcp  open  ssl/realserver?
|_ ssl-date: TLS randomness does not represent time
8080/tcp  open  http         nginx 1.14.0 (Ubuntu)
|_ http-methods:
|_ Supported Methods: GET HEAD POST
|_ http-server-header: nginx/1.14.0 (Ubuntu)
|_ http-title: 403 Forbidden
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=8/28%OT=22%CT=1%CU=36262%PV=Y%DS=2%DC=T%G=Y%TM=5F49524
OS:C%P=x86_64-pc-linux-gnu)SEQ(SP=13%GCD=FA00%ISR=AF%II=I%TS=U)SEQ(SP=11%GC
OS:D=FA00%ISR=AF%CI=I%II=I%TS=U)SEQ(SP=17%GCD=FA00%ISR=AF%TS=U)OPS(O1=M5B4%
```