DNS PACKET ANALYSIS USING WIREHARK

BY

SOMKENE RICHARD

19th SEPTEMBER, 2024

EXECUTIVE SUMMARY

An analysis was conducted on a randomly selected packet from a provided DNS.cap file to evaluate its network traffic which occurred on 2005/03/30 at 08:51 am. This analysis focused on identifying the domain queried and the type of response received. The findings suggest that the error observed may be attributed to the client querying either an incorrectly spelled domain or a domain that does not exist.

INTRODUCTION

DNS packet analysis involves examining the details of a DNS traffic as it flows across as a network using some cybersecurity tools. This type of analysis is mostly done to understand, troubleshoot, and ensure the proper functioning of DNS operations within a network.

TOOLS

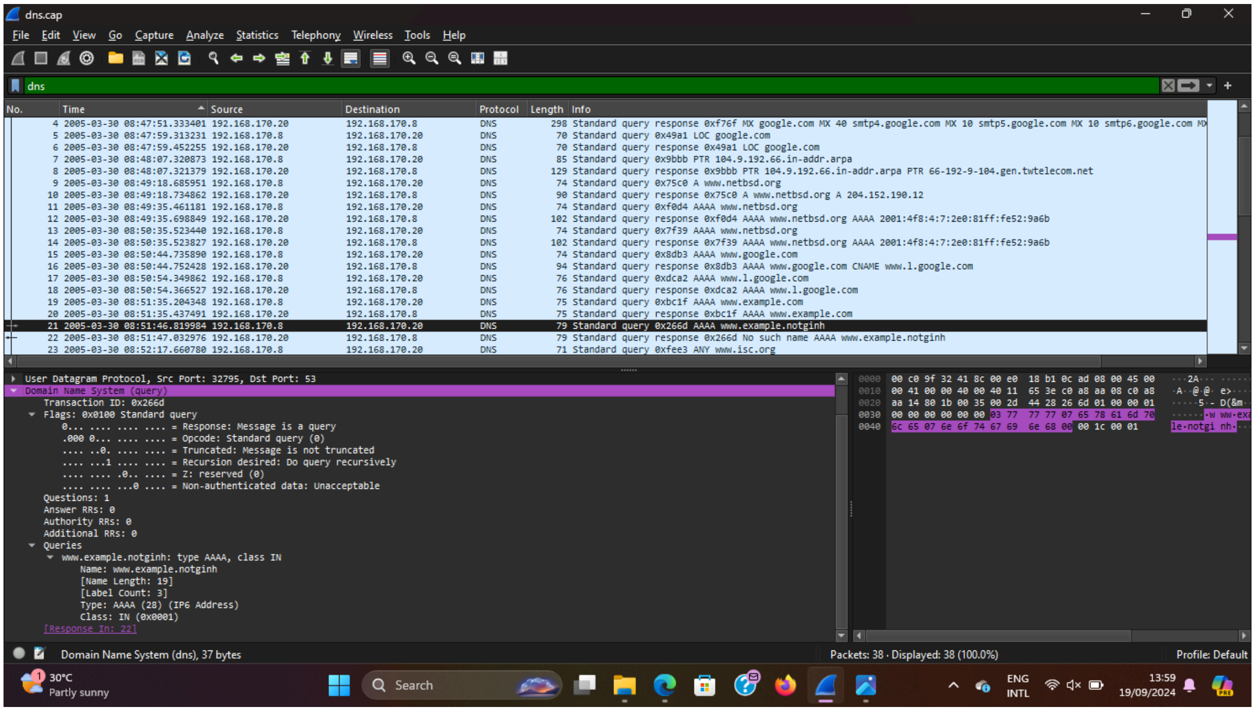
1.Hp laptop: device used for the analysis

2. Wireshark: used to view the captured DNS packets and its details

3. Virustotal: for scanning the IP addresses

4. Pen and paper: for recording findings

ANALYSIS



dns.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time                        Source          Destination     Protocol Length Info
   4 2005-03-30 08:47:51.333401 192.168.170.20  192.168.170.8   DNS       298 Standard query response 0xf76f MX google.com MX 40 smtp4.google.com MX 10 smtp5.google.com MX 10 smtp6.google.com MX
   5 2005-03-30 08:47:59.313231 192.168.170.8   192.168.170.20  DNS        70 Standard query 0x49a1 LOC google.com
   6 2005-03-30 08:47:59.452255 192.168.170.20  192.168.170.8   DNS        70 Standard query response 0x49a1 LOC google.com
   7 2005-03-30 08:48:07.320873 192.168.170.8   192.168.170.20  DNS        85 Standard query 0x9bbb PTR 104.9.192.66.in-addr.arpa
   8 2005-03-30 08:48:07.321379 192.168.170.20  192.168.170.8   DNS       129 Standard query response 0x9bbb PTR 104.9.192.66.in-addr.arpa PTR 66-192-9-104.gen.twtelecom.net
   9 2005-03-30 08:49:18.685951 192.168.170.8   192.168.170.20  DNS        74 Standard query 0x75c0 A www.netbsd.org
  10 2005-03-30 08:49:18.734862 192.168.170.20  192.168.170.8   DNS        90 Standard query response 0x75c0 A www.netbsd.org A 204.152.190.12
  11 2005-03-30 08:49:35.461181 192.168.170.8   192.168.170.20  DNS        74 Standard query 0xf0d4 AAAA www.netbsd.org
  12 2005-03-30 08:49:35.698849 192.168.170.20  192.168.170.8   DNS       102 Standard query response 0xf0d4 AAAA www.netbsd.org AAAA 2001:4f8:4:7:2e0:81ff:fe52:9a6b
  13 2005-03-30 08:50:35.523440 192.168.170.8   192.168.170.20  DNS        74 Standard query 0x7f39 AAAA www.netbsd.org
  14 2005-03-30 08:50:35.523827 192.168.170.20  192.168.170.8   DNS       102 Standard query response 0x7f39 AAAA www.netbsd.org AAAA 2001:4f8:4:7:2e0:81ff:fe52:9a6b
  15 2005-03-30 08:50:44.735890 192.168.170.8   192.168.170.20  DNS        74 Standard query 0x8db3 AAAA www.google.com
  16 2005-03-30 08:50:44.752428 192.168.170.20  192.168.170.8   DNS        94 Standard query response 0x8db3 AAAA www.google.com CNAME www.l.google.com
  17 2005-03-30 08:50:54.349862 192.168.170.8   192.168.170.20  DNS        76 Standard query 0xdca2 AAAA www.l.google.com
  18 2005-03-30 08:50:54.366527 192.168.170.20  192.168.170.8   DNS        76 Standard query response 0xdca2 AAAA www.l.google.com
  19 2005-03-30 08:51:35.204348 192.168.170.8   192.168.170.20  DNS        75 Standard query 0xbc1f AAAA www.example.com
  20 2005-03-30 08:51:35.437491 192.168.170.20  192.168.170.8   DNS        75 Standard query response 0xbc1f AAAA www.example.com
  21 2005-03-30 08:51:46.819984 192.168.170.8   192.168.170.20  DNS        79 Standard query 0x266d AAAA www.example.notginh
  22 2005-03-30 08:51:47.032976 192.168.170.20  192.168.170.8   DNS        79 Standard query response 0x266d No such name AAAA www.example.notginh
  23 2005-03-30 08:52:17.660780 192.168.170.8   192.168.170.20  DNS        71 Standard query 0xfee3 ANY www.isc.org
```

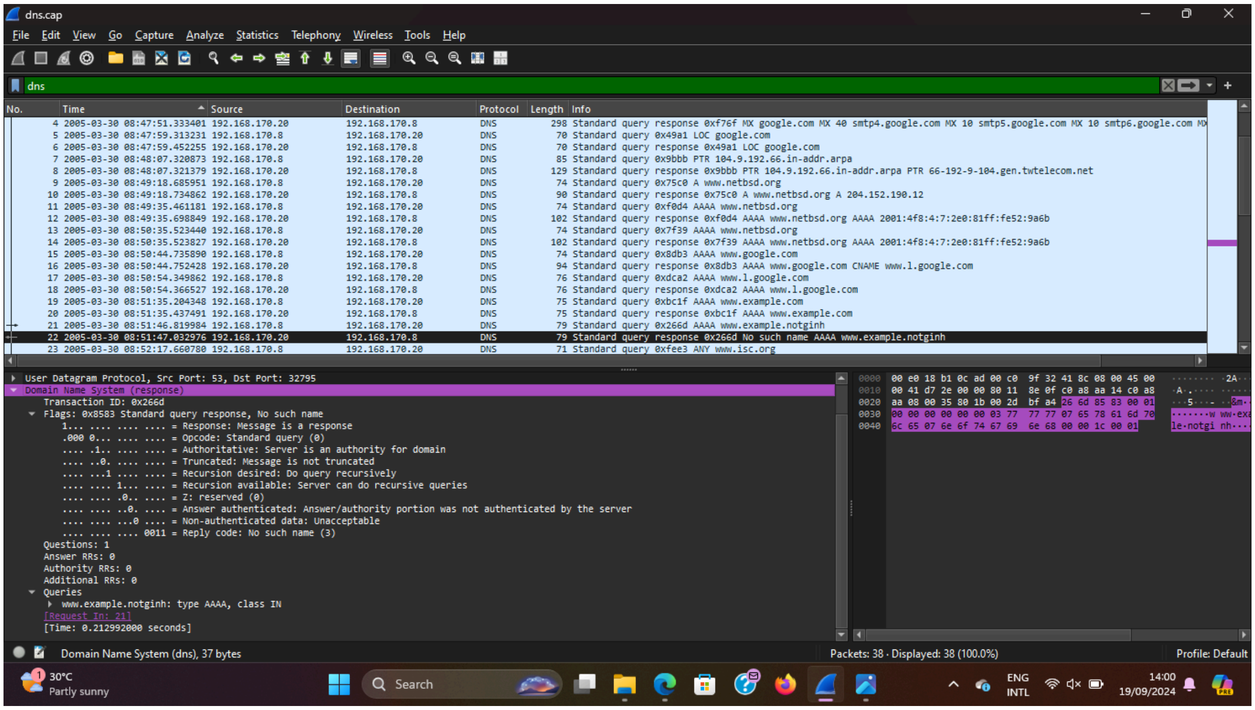
```
> User Datagram Protocol, Src Port: 32795, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x266d
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.example.notginh: type AAAA, class IN
        Name: www.example.notginh
        [Name Length: 19]
        [Label Count: 3]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
    [Response In: 22]
```

```
0000  00 c0 9f 32 41 8c 00 e0  18 b1 0c ad 08 00 45 00   ···2A··· ······
0010  00 41 00 00 40 00 40 11  65 3e c0 a8 aa 08 c0 a8   ·A··@·@· e>····
0020  aa 14 80 1b 00 35 00 2d  44 28 26 6d 01 00 00 01   ·····5·- D(&m··
0030  00 00 00 00 00 00 03 77  77 77 07 65 78 61 6d 70   ·······w ww·exa
0040  6c 65 07 6e 6f 74 67 69  6e 68 00 00 1c 00 01      le·notgi nh····
```

```
Domain Name System (dns), 37 bytes          Packets: 38 · Displayed: 38 (100.0%)          Profile: Default
```

Fig 1: packet query details

From the image in Fig 1, it was seen that the queried domain (www.example.notginh) was mapped to an Ipv6 address hence the reason for the "type AAAA”



```
No.   Time                        Source           Destination      Protocol Length Info
    4 2005-03-30 08:47:51.333401 192.168.170.20   192.168.170.8    DNS         298 Standard query response 0xf76f MX google.com MX 40 smtp4.google.com MX 10 smtp5.google.com MX 10 smtp6.google.com MX
    5 2005-03-30 08:47:59.313231 192.168.170.8    192.168.170.20   DNS          70 Standard query 0x49a1 LOC google.com
    6 2005-03-30 08:47:59.452255 192.168.170.20   192.168.170.8    DNS          70 Standard query response 0x49a1 LOC google.com
    7 2005-03-30 08:48:07.320873 192.168.170.8    192.168.170.20   DNS          85 Standard query 0x9bbb PTR 104.9.192.66.in-addr.arpa
    8 2005-03-30 08:48:07.321379 192.168.170.20   192.168.170.8    DNS         129 Standard query response 0x9bbb PTR 104.9.192.66.in-addr.arpa PTR 66-192-9-104.gen.twtelecom.net
    9 2005-03-30 08:49:18.685951 192.168.170.8    192.168.170.20   DNS          74 Standard query 0x75c0 A www.netbsd.org
   10 2005-03-30 08:49:18.734862 192.168.170.20   192.168.170.8    DNS          90 Standard query response 0x75c0 A www.netbsd.org A 204.152.190.12
   11 2005-03-30 08:49:35.461181 192.168.170.8    192.168.170.20   DNS          74 Standard query 0xf0d4 AAAA www.netbsd.org
   12 2005-03-30 08:49:35.698849 192.168.170.20   192.168.170.8    DNS         102 Standard query response 0xf0d4 AAAA www.netbsd.org AAAA 2001:4f8:4:7:2e0:81ff:fe52:9a6b
   13 2005-03-30 08:50:35.523440 192.168.170.8    192.168.170.20   DNS          74 Standard query 0x7f39 AAAA www.netbsd.org
   14 2005-03-30 08:50:35.523827 192.168.170.20   192.168.170.8    DNS         102 Standard query response 0x7f39 AAAA www.netbsd.org AAAA 2001:4f8:4:7:2e0:81ff:fe52:9a6b
   15 2005-03-30 08:50:44.735890 192.168.170.8    192.168.170.20   DNS          74 Standard query 0x8db3 AAAA www.google.com
   16 2005-03-30 08:50:44.752428 192.168.170.20   192.168.170.8    DNS          94 Standard query response 0x8db3 AAAA www.google.com CNAME www.l.google.com
   17 2005-03-30 08:50:54.349862 192.168.170.8    192.168.170.20   DNS          76 Standard query 0xdca2 AAAA www.l.google.com
   18 2005-03-30 08:50:54.366527 192.168.170.20   192.168.170.8    DNS          76 Standard query response 0xdca2 AAAA www.l.google.com
   19 2005-03-30 08:51:35.204348 192.168.170.8    192.168.170.20   DNS          75 Standard query 0xbc1f AAAA www.example.com
   20 2005-03-30 08:51:35.437491 192.168.170.20   192.168.170.8    DNS          75 Standard query response 0xbc1f AAAA www.example.com
   21 2005-03-30 08:51:46.819984 192.168.170.8    192.168.170.20   DNS          79 Standard query 0x266d AAAA www.example.notginh
   22 2005-03-30 08:51:47.032976 192.168.170.20   192.168.170.8    DNS          79 Standard query response 0x266d No such name AAAA www.example.notginh
   23 2005-03-30 08:52:17.660780 192.168.170.8    192.168.170.20   DNS          71 Standard query 0xfee3 ANY www.isc.org
```

```
User Datagram Protocol, Src Port: 53, Dst Port: 32795
Domain Name System (response)
    Transaction ID: 0x266d
    Flags: 0x8583 Standard query response, No such name
        1... .... .... .... = Response: Message is a response
        .000 0... .... .... = Opcode: Standard query (0)
        .... .1.. .... .... = Authoritative: Server is an authority for domain
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... 1... .... = Recursion available: Server can do recursive queries
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0011 = Reply code: No such name (3)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.example.notginh: type AAAA, class IN
    [Request In: 21]
    [Time: 0.212992000 seconds]
```

```
0000  00 e0 18 b1 0c ad 00 c0  9f 32 41 8c 08 00 45 00   ········ ·2A·
0010  00 41 d7 2e 00 00 80 11  8e 0f c0 a8 aa 14 c0 a8   ·A·.···· ····
0020  aa 08 00 35 80 1b 00 2d  bf a4 26 6d 85 83 00 01   ···5···- ··&m·
0030  00 00 00 00 00 00 03 77  77 77 07 65 78 61 6d 70   ·······w ww·exa
0040  6c 65 07 6e 6f 74 67 69  6e 68 00 00 1c 00 01      le·notgi nh···
```

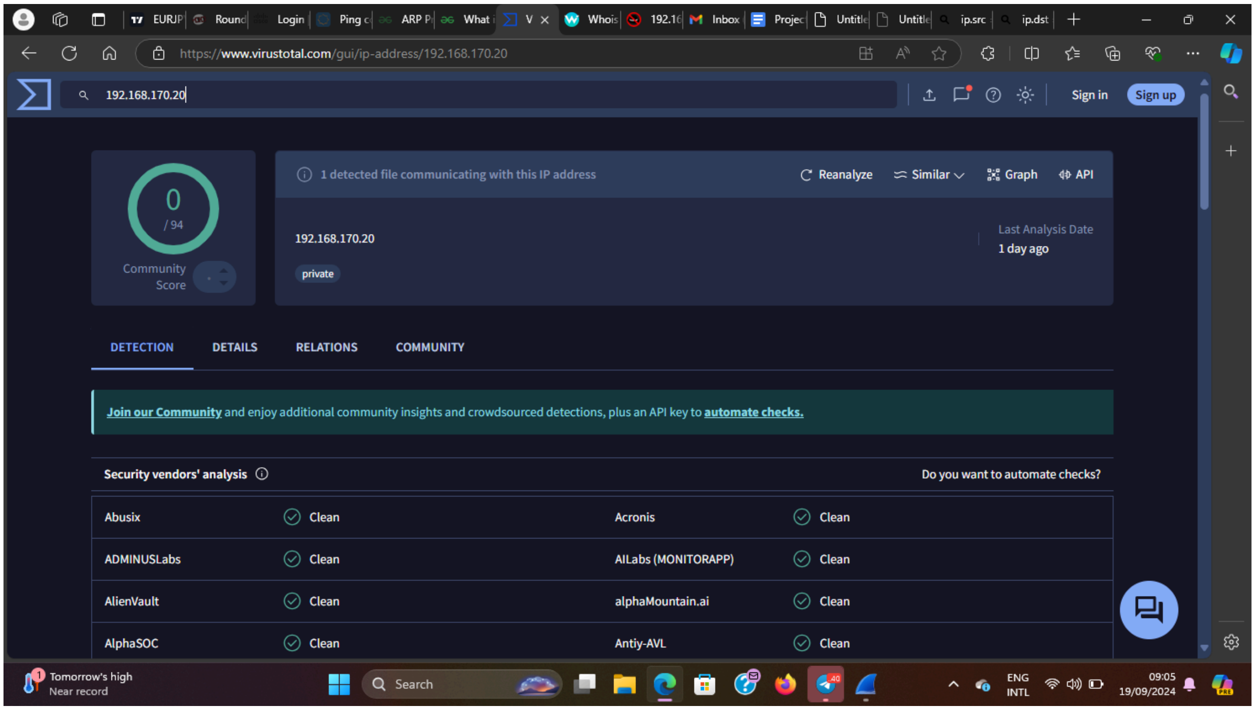
Domain Name System (dns), 37 bytes

Packets: 38 · Displayed: 38 (100.0%)

Profile: Default

Fig 2: packet response details

From the image in Fig 2, the response from the queried domain was given as "NO such name" which indicates an error in the domain.



192.168.170.20

0
/ 94
Community Score

1 detected file communicating with this IP address

Reanalyze | Similar | Graph | API

192.168.170.20

private

Last Analysis Date
1 day ago

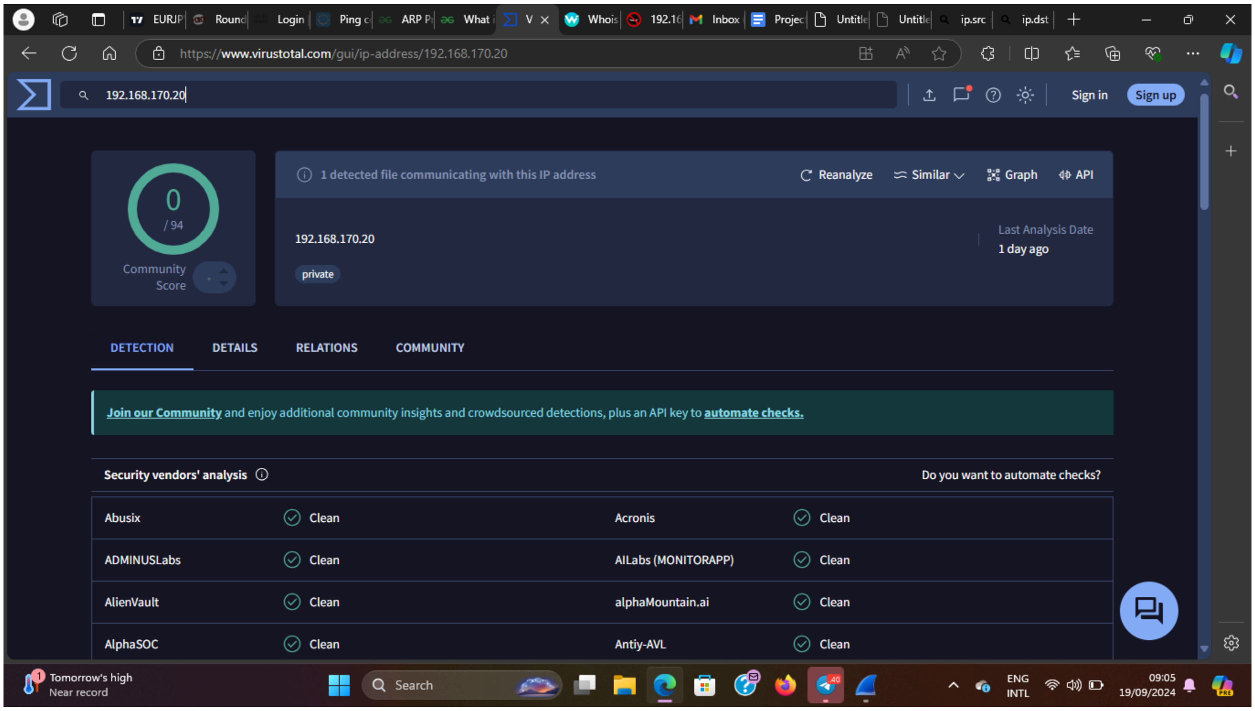
DETECTION | DETAILS | RELATIONS | COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis | Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
AlphaSOC	✓ Clean	Antiy-AVL	✓ Clean

Fig 3: scanning of the source IP address



192.168.170.20

0
/ 94
Community Score

1 detected file communicating with this IP address

Reanalyze | Similar | Graph | API

192.168.170.20

private

Last Analysis Date
1 day ago

DETECTION | DETAILS | RELATIONS | COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis | Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
AlphaSOC	✓ Clean	Antiy-AVL	✓ Clean

Fig 4: scanning of the destination IP address

Further scanning of the source and destination IP addresses (which happens to be IPv4) as seen in *Fig 3 & 4* was shown to have been a private Network (VPN).

CONCLUSION

A client on a private network queried an incorrect or non-existing domain. I recommend double-checking the domain name for any typographical errors. If the domain still cannot be found, it may either be unregistered or could have been deleted.