

Polytechnic University of Puerto Rico
Electrical and Computer Engineering & Computer Science Department
COE 4330, Section 80 – Computer Networks

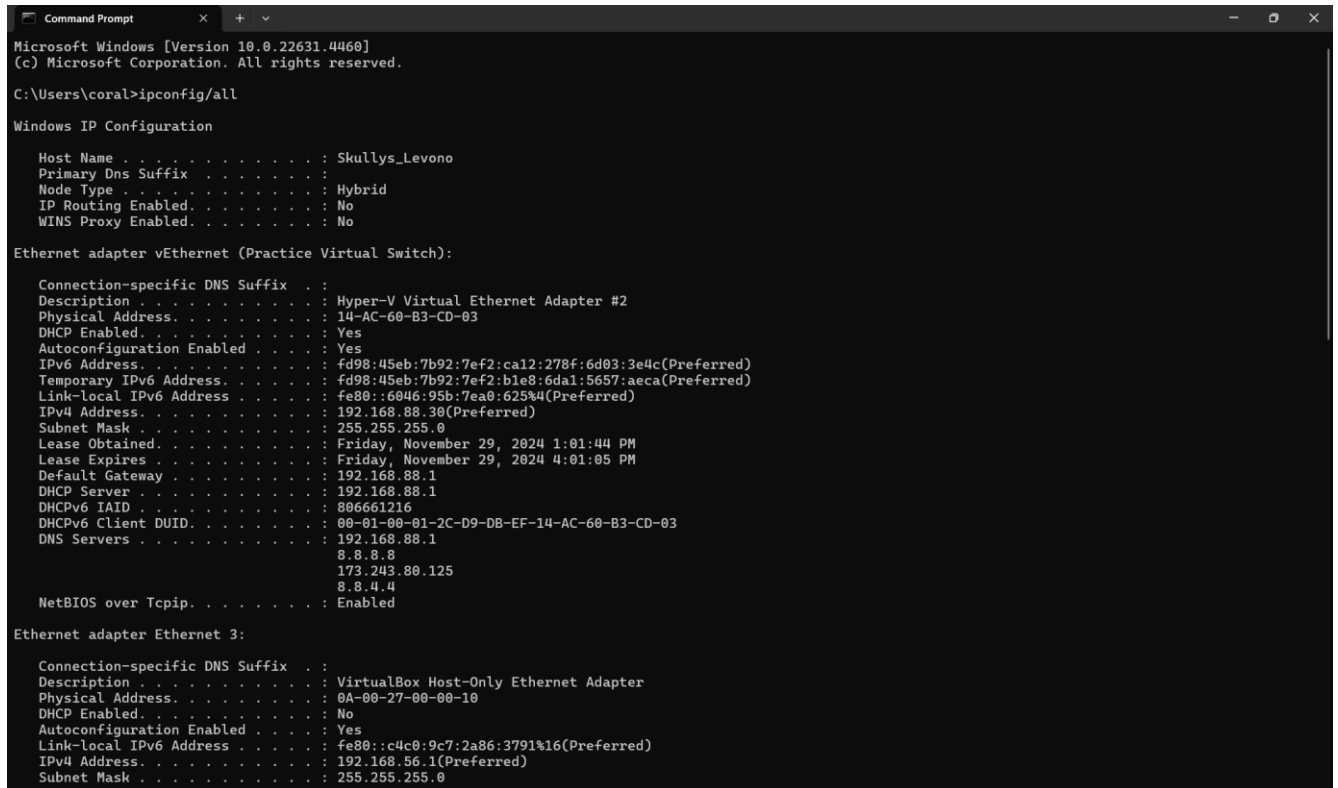
Homework 3

Name: Coral S. Schmidt Montilla

ID#: 148830

Completely answer all of the following questions.

1. Open Windows' Command Prompt and type ipconfig /all (in Linux/Unix/Mac type ifconfig). Provide a screenshot that shows the result of executing the command for the network interface in use during the exercise. This screenshot will show your computer's IP address, default gateway, and local DNS servers. *1 point*



```
Microsoft Windows [Version 10.0.22631.4460]
(c) Microsoft Corporation. All rights reserved.

C:\Users\coral>ipconfig/all

Windows IP Configuration

Host Name . . . . . : Skullys_Levono
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter vEthernet (Practice Virtual Switch):

Connection-specific DNS Suffix . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter #2
Physical Address. . . . . : 14-AC-60-B3-CD-03
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : fd98:45eb:7b92:7ef2:ca12:278f:6d03:3e4c(Preferred)
Temporary IPv6 Address. . . . . : fd98:45eb:7b92:7ef2:b1e8:6dal:5657:aeca(Preferred)
Link-local IPv6 Address . . . . . : fe80::6046:95b:7ea0:625%4(Preferred)
IPv4 Address. . . . . : 192.168.88.30(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, November 29, 2024 1:01:44 PM
Lease Expires . . . . . : Friday, November 29, 2024 4:01:05 PM
Default Gateway . . . . . : 192.168.88.1
DHCP Server . . . . . : 192.168.88.1
DHCPv6 IAID . . . . . : 806661216
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-D9-DB-EF-14-AC-60-B3-CD-03
DNS Servers . . . . . : 192.168.88.1
                        8.8.8.8
                        173.243.80.125
                        8.8.4.4
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Ethernet 3:

Connection-specific DNS Suffix . :
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-10
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c4c0:9c7:2a86:3791%16(Preferred)
IPv4 Address. . . . . : 192.168.56.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
```

Polytechnic University of Puerto Rico
Electrical and Computer Engineering & Computer Science Department
COE 4330, Section 80 – Computer Networks

```
Command Prompt
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 1074397223
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-D9-DB-EF-14-AC-60-B3-CD-03
NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 16-AC-60-B3-ED-23
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 16-AC-60-B3-FD-33
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::28a3:11e8:92b3:92f7%5(Preferred)
IPv4 Address. . . . . : 192.168.137.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : 14-AC-60-B3-CD-04
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter vEthernet (Default Switch):

Connection-specific DNS Suffix . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter
Physical Address. . . . . : 00-15-5D-AC-D7-5A
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::47ad:65c3:43ad:a8e8%27(Preferred)
IPv4 Address. . . . . : 172.23.224.1(Preferred)
Subnet Mask . . . . . : 255.255.240.0
```

```
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 452990301
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-D9-DB-EF-14-AC-60-B3-CD-03
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\coral>
```

2. Run nslookup to obtain the IP address of the University's web site, www.pupr.edu. Include a screenshot to justify your answer. *1 point*

As you can see from the screenshot below, the IP address of www.pupr.edu is **167.172.0.84**.

```
Command Prompt
Microsoft Windows [Version 10.0.22631.4460]
(c) Microsoft Corporation. All rights reserved.

C:\Users\coral>nslookup www.pupr.edu
Server: router.lan
Address: 192.168.88.1

Non-authoritative answer:
Name: www.pupr.edu
Address: 167.172.0.84
```

3. Run nslookup to determine the authoritative DNS servers for www.pupr.edu. Include a screenshot to justify your answer. *1 point*

As you can see from the screenshot below, the authoritative DNS servers for www.pupr.edu are **ns1-37.azure-dns.com, ns2-37.azure-dns.net, ns3-37.azure-dns.org, and ns4-37.azure-dns.info.**

```
C:\Users\coral>nslookup -type=ns www.pupr.edu
Server:  router.lan
Address:  192.168.88.1

*** No name server (NS) records available for www.pupr.edu

C:\Users\coral>nslookup -type=ns pupr.edu
Server:  router.lan
Address:  192.168.88.1

Non-authoritative answer:
pupr.edu      nameserver = ns3-37.azure-dns.org
pupr.edu      nameserver = ns4-37.azure-dns.info
pupr.edu      nameserver = ns1-37.azure-dns.com
pupr.edu      nameserver = ns2-37.azure-dns.net

pupr.edu      nameserver = ns4-37.azure-dns.info
pupr.edu      nameserver = ns1-37.azure-dns.com
pupr.edu      nameserver = ns2-37.azure-dns.net
pupr.edu      nameserver = ns3-37.azure-dns.org
```

4. Run nslookup to determine the mail servers for www.pupr.edu. Include a screenshot to justify your answer. *1 point*

As you can see from the screenshot below, the mail server for www.pupr.edu is **pupr-edu.mail.protection.outlook.com with an MX preference of 10.**

```
C:\Users\coral>nslookup -type=mx pupr.edu
Server:  router.lan
Address:  192.168.88.1

Non-authoritative answer:
pupr.edu      MX preference = 10, mail exchanger = pupr-edu.mail.protection.outlook.com

pupr.edu      nameserver = ns3-37.azure-dns.org
pupr.edu      nameserver = ns4-37.azure-dns.info
pupr.edu      nameserver = ns1-37.azure-dns.com
pupr.edu      nameserver = ns2-37.azure-dns.net
```

Polytechnic University of Puerto Rico
Electrical and Computer Engineering & Computer Science Department
COE 4330, Section 80 – Computer Networks

Complete the lab's Part 3 before answering the following questions.

5. What is the IP address of your computer? Include a screenshot to justify your answer. *1 point*

As you can see from the screenshot below, the IP address of my computer is **192.168.88.30**.

```
C:\Users\coral>ipconfig

Windows IP Configuration

Ethernet adapter vEthernet (Practice Virtual Switch):

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : fd98:45eb:7b92:7ef2:ca12:278f:6d03:3e4c
    Temporary IPv6 Address. . . . . : fd98:45eb:7b92:7ef2:b1e8:6da1:5657:aeca
    Link-local IPv6 Address . . . . . : fe80::6046:95b:7ea0:625%4
    IPv4 Address. . . . . : 192.168.88.30
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.88.1
```

6. Locate the DNS query and response messages. Are then sent over UDP or TCP? Include a Wireshark screenshot to justify your answer. *1 point*

As you can see from the screenshot below, the DNS query and response messages are sent over **UDP**. This can be observed in the packet details section, where the User Datagram **Protocol (UDP)** is specified as the transport protocol.

The screenshot shows the Wireshark network protocol analyzer. The top pane displays a list of captured packets, with DNS traffic highlighted. The middle pane shows the details of the selected packet (No. 342), which is a 'Standard query response' from 192.168.88.1 to 192.168.88.30. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
394	4.329739	192.168.88.30	192.168.88.1	DNS	80	Standard query 0xa4d8 A catalog.gamepass.com
395	4.329837	192.168.88.30	192.168.88.1	DNS	80	Standard query 0xa4d7 AAAA catalog.gamepass.com
396	4.405502	192.168.88.1	192.168.88.30	DNS	192	Standard query response 0xa4d8 A catalog.gamepass.com CNAME catalog.gamepass.com.edgesuite.net CNAME a1992.dscd.aka
397	4.410382	192.168.88.1	192.168.88.30	DNS	280	Standard query response 0xa4d7 AAAA catalog.gamepass.com CNAME catalog.gamepass.com.edgesuite.net CNAME a1992.dscd.
3415	11.802139	192.168.88.30	192.168.88.1	DNS	83	Standard query 0xa274 A www.msftconnecttest.com
3416	11.802238	192.168.88.30	192.168.88.1	DNS	83	Standard query 0x57d4 AAAA www.msftconnecttest.com
3417	11.864951	192.168.88.1	192.168.88.30	DNS	83	Standard query response 0x57d4 AAAA www.msftconnecttest.com
3420	11.800024	192.168.88.1	192.168.88.30	DNS	227	Standard query response 0xa274 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.e
3633	13.302991	192.168.88.30	192.168.88.1	DNS	74	Standard query 0xd351 A ecs.office.com
3634	13.303084	192.168.88.30	192.168.88.1	DNS	74	Standard query 0xf491 AAAA ecs.office.com
3650	13.366893	192.168.88.1	192.168.88.30	DNS	305	Standard query response 0xf491 AAAA ecs.office.com CNAME ecs.office.trafficmanager.net CNAME s-0005-office.config.s
3651	13.368626	192.168.88.1	192.168.88.30	DNS	229	Standard query response 0xd351 A ecs.office.com CNAME ecs.office.trafficmanager.net CNAME s-0005-office.config.skyp
3925	14.052600	192.168.88.30	192.168.88.1	DNS	101	Standard query 0xa80 A msedge.b.tlu.dl.delivery.mp.microsoft.com
3926	14.052600	192.168.88.30	192.168.88.1	DNS	101	Standard query 0x3d94 AAAA msedge.b.tlu.dl.delivery.mp.microsoft.com
4022	14.119491	192.168.88.1	192.168.88.30	DNS	304	Standard query response 0x3d94 AAAA msedge.b.tlu.dl.delivery.mp.microsoft.com CNAME star.b.tlu.dl.delivery.mp.micro
4133	14.146280	192.168.88.1	192.168.88.30	DNS	342	Standard query response 0xa80 A msedge.b.tlu.dl.delivery.mp.microsoft.com CNAME star.b.tlu.dl.delivery.mp.microsof

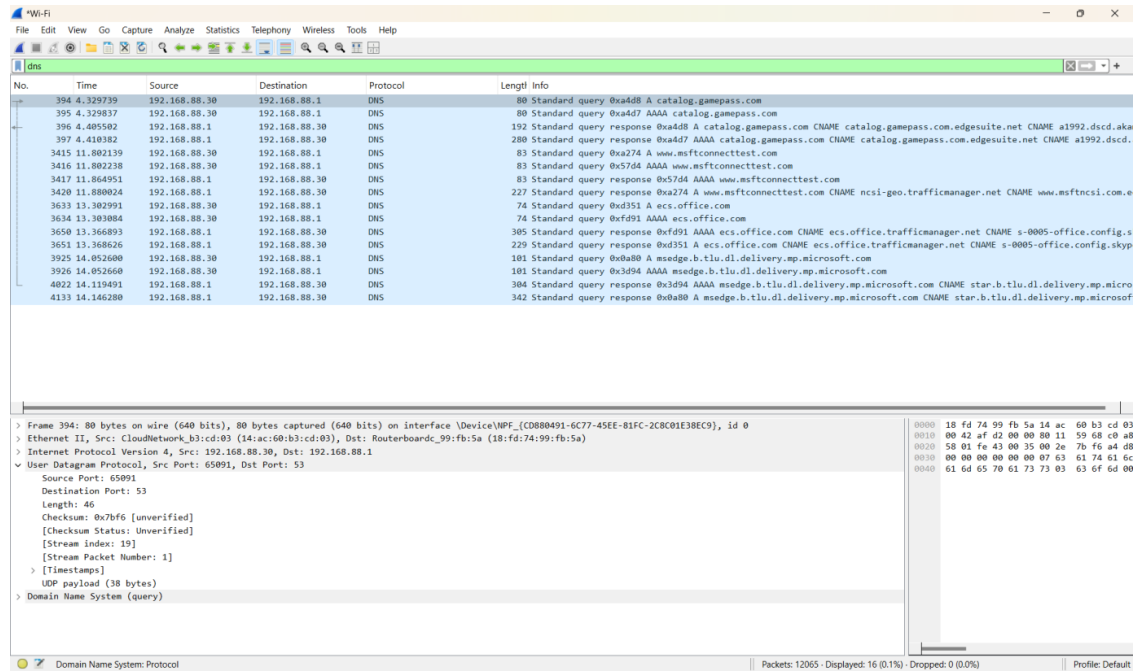
Frame 394: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF{C0880491-6C77-45EE-81FC-2C8C01E38EC9}, id 0
> Ethernet II, Src: CloudNetwork_b3:cd:03 (14:ac:60:b3:cd:03), Dst: Routerboard_99:fb:5a (18:fd:74:99:fb:5a)
> Internet Protocol Version 4, Src: 192.168.88.30, Dst: 192.168.88.1
> User Datagram Protocol, Src Port: 65891, Dst Port: 53
 Source Port: 65891
 Destination Port: 53
 Length: 46
 Checksum: 0x7b6f [unverified]
 [Checksum Status: Unverified]
 [Stream Index: 19]
 [Stream Packet Number: 1]
 > [Timestamp]
 UDP payload (38 bytes)
 > Domain Name System (query)

Polytechnic University of Puerto Rico
Electrical and Computer Engineering & Computer Science Department
COE 4330, Section 80 – Computer Networks

7. What is the destination port for the DNS query message? Include a Wireshark screenshot to justify your answer. *1 point*

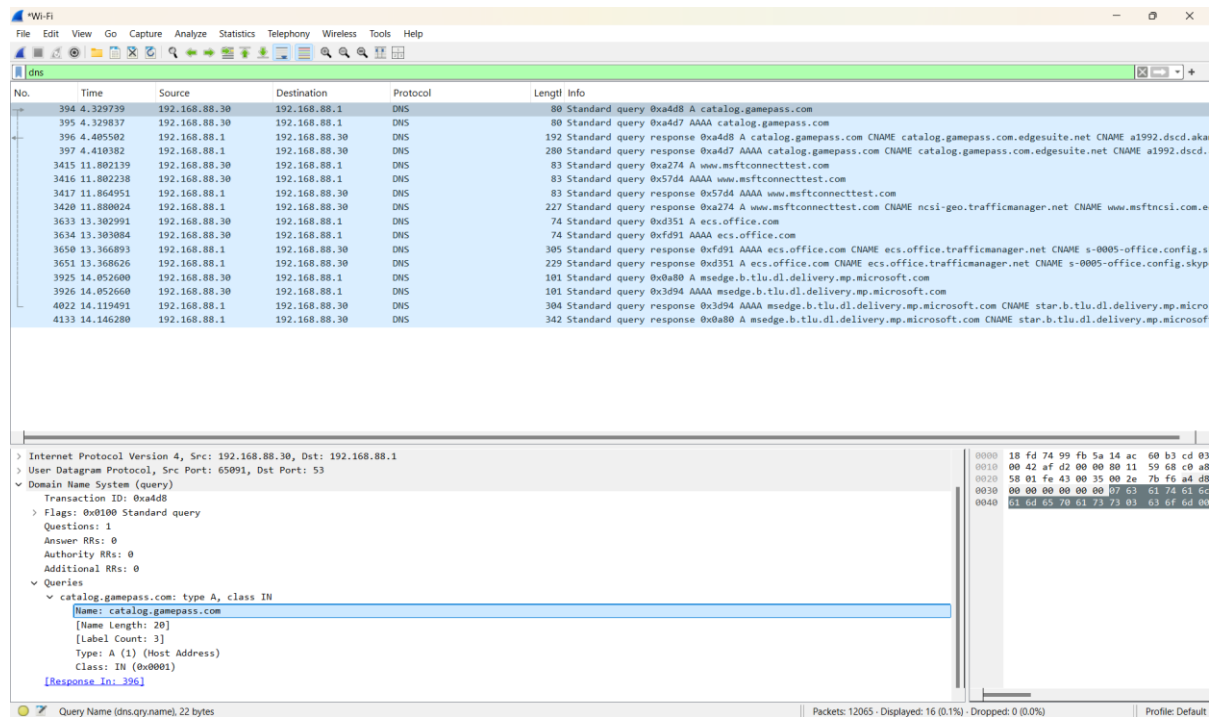
As you can see from the screenshot below, the destination port for the DNS query message is

53.



8. Examine the DNS query message. What “Type” of DNS query is it? Include a Wireshark screenshot to justify your answer. *1 point*

As you can see from the screenshot below, the DNS query message is of **Type A (Host Address)**.



Polytechnic University of Puerto Rico
Electrical and Computer Engineering & Computer Science Department
COE 4330, Section 80 – Computer Networks

9. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? Include a Wireshark screenshot to justify your answer. *2 points*

As you can see from the screenshot below, the DNS response message provides **4 answers**. Each answer contains the following:

1. catalog.gamepass.com: CNAME, alias for catalog.gamepass.com.edgesuite.net.
2. catalog.gamepass.com.edgesuite.net: CNAME, alias for a1992.dscd.akamai.net.
3. a1992.dscd.akamai.net: Type A, IPv4 address 23.39.210.17.
4. a1992.dscd.akamai.net: Type A, IPv4 address 23.39.210.18.

These records represent a chain of aliases (CNAME) and two IPv4 addresses (A records) that resolve to the requested hostname.

The screenshot shows a Wireshark capture of a DNS response. The packet list pane displays a list of packets, with packet 396 selected. The details pane shows the structure of the DNS response, including the transaction ID, flags, questions, and answers. The answers section lists four records: two CNAME records and two A records.

No.	Time	Source	Destination	Protocol	Length	Info
394	4.329739	192.168.88.30	192.168.88.1	DNS	80	Standard query 0xa4d8 A catalog.gamepass.com
395	4.329837	192.168.88.30	192.168.88.1	DNS	80	Standard query 0xa4d7 AAAA catalog.gamepass.com
396	4.405502	192.168.88.1	192.168.88.30	DNS	192	Standard query response 0xa4d8 A catalog.gamepass.com CNAME catalog.gamepass.com.edgesuite.net CNAME a1992.dscd.akamai.net

Frame 396: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits) on interface \Device\NPF_{C0880491-6C77-45EE-81FC-2C8C01E38EC9}, id 0

Ethernet II, Src: Routerboardc_99:fb:5a (18:fd:74:99:fb:5a), Dst: CloudNetwork_b3:cd:03 (14:ac:60:b3:cd:03)

Internet Protocol Version 4, Src: 192.168.88.1, Dst: 192.168.88.30

User Datagram Protocol, Src Port: 53, Dst Port: 65091

Domain Name System (response)

Transaction ID: 0xa4d8

Flags: 0x1800 Standard query response, No error

Questions: 1

Answer RRs: 4

Authority RRs: 0

Additional RRs: 0

Queries

- catalog.gamepass.com: type A, class IN
- Name: catalog.gamepass.com
- Name Length: 20
- Label Count: 3
- Type: A (1) (Host Address)
- Class: IN (0x0001)

Answers

- catalog.gamepass.com: type CNAME, class IN, cname catalog.gamepass.com.edgesuite.net
- catalog.gamepass.com.edgesuite.net: type CNAME, class IN, cname a1992.dscd.akamai.net
- a1992.dscd.akamai.net: type A, class IN, addr 23.39.210.17
- a1992.dscd.akamai.net: type A, class IN, addr 23.39.210.18

[Request In: 394]

[Time: 0.075763000 seconds]