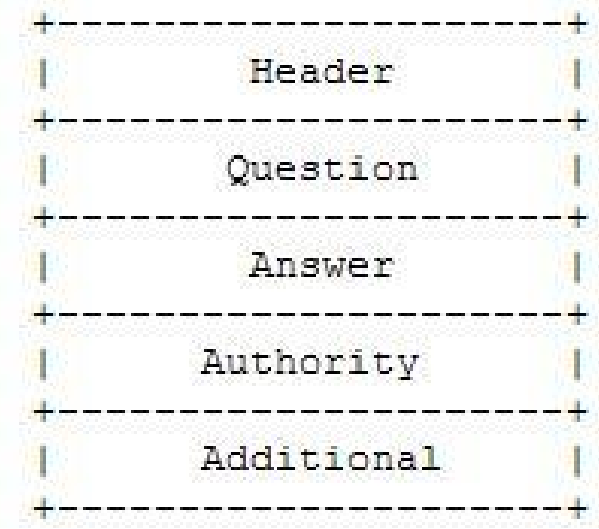
Message DNS

Format du message DNS

- Entête : spécifie le type du message (taille fixe: 12 octets)
- Question : zone réservée à la question posée au serveur de noms
- Réponse: zone réservée à la réponse
- Autorité: contient les informations sur les serveurs de noms
- Additionnel: contient des informations additionnelles.



Champs entête (header)

- ID: identifiant est un entier permettant d'identifier la requête.
- Champ paramètres (Flags) contient les champs suivant:

-- QR (1 bit): indique si le message est une question (0) ou une réponse (1).

-- OPCODE (4 bits): type de la requête (0000 pour une requête simple).

-- AA (1 bit): le serveur qui a fourni la réponse a-t'il autorité sur le domaine?

-- TC (1 bit): indique si le message est tronqué.

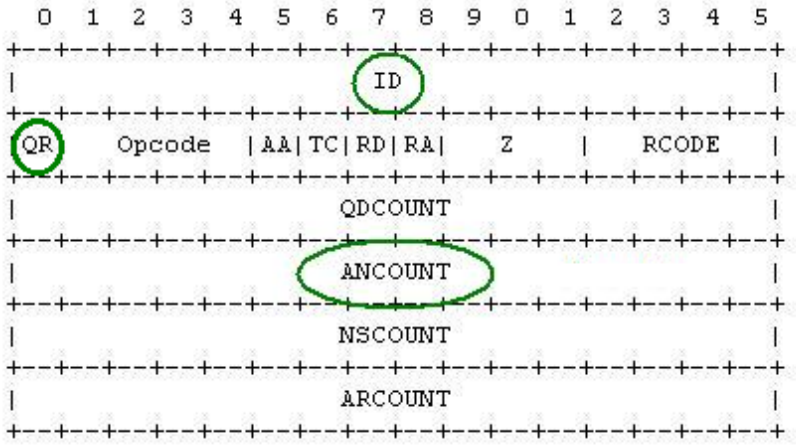
-- RD (1 bit): demande d'une requête récursive.

-- RA (1 bit): indique que le serveur peut faire une demande récursive.

-- UNUSED, AD, CD (1 bit chacun): non utilisés.

-- RCODE (4 bits): code de retour. 0: OK, 1: erreur sur le format de la requête, 2: problème du serveur, 3: nom de domaine non trouvé (valide seulement si AA), 4: requête non supportée, 5: le serveur refuse de répondre (raisons de sécurité ou autres).

- QDCount: nombre de questions.
- ANCount, NSCount, ARCount: nombre d'entrées dans les champs "Réponse", "Autorité", "Additionnel".



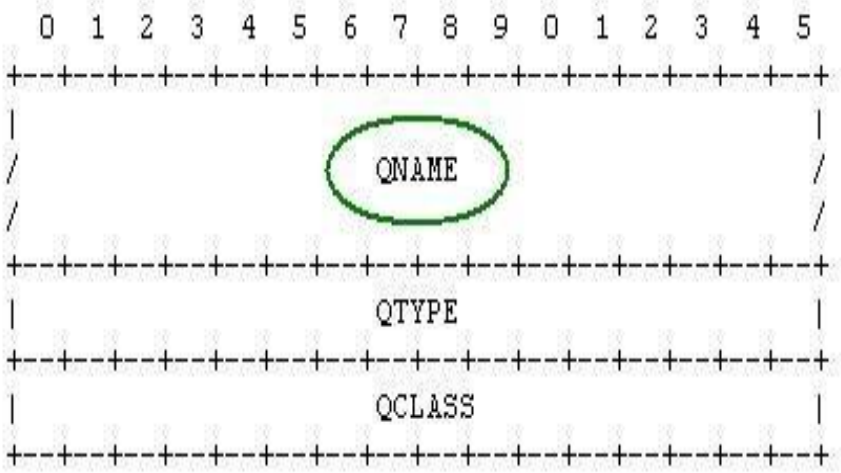
Champ Question

- QNAME: les différentes sections du nom de domaine recherché, chacune précédée par un octet représentant le nombre de caractères que cette section contient. L'octet 00 pour indiquer la fin du nom.
- Type (16 bits) pour indiquer le type de la requête.

  Ex:0x0001 pour A records

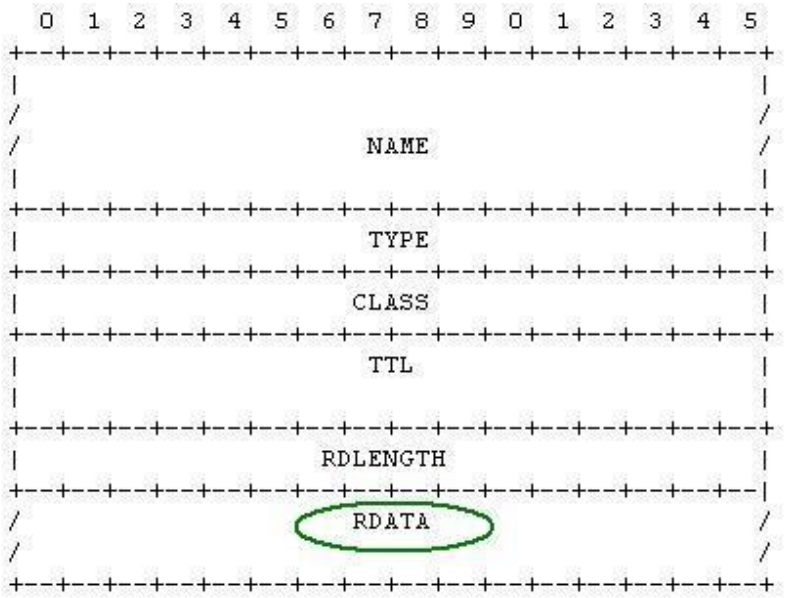
  0x0005 pour les CNAME
- Class (16 bits) indique le type du protocole.

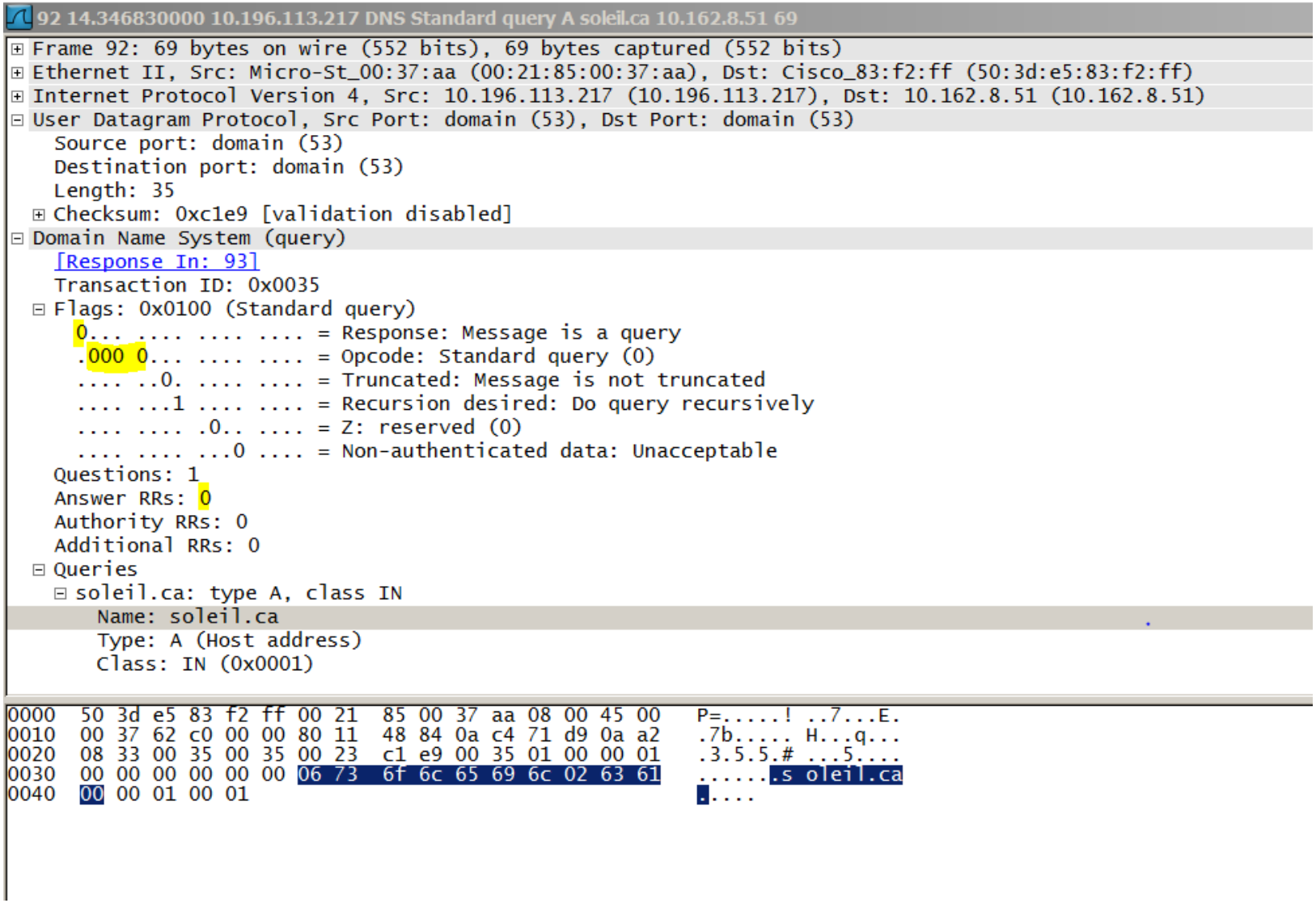
  Ex: 0x0001 pour IN (Internet Adr)

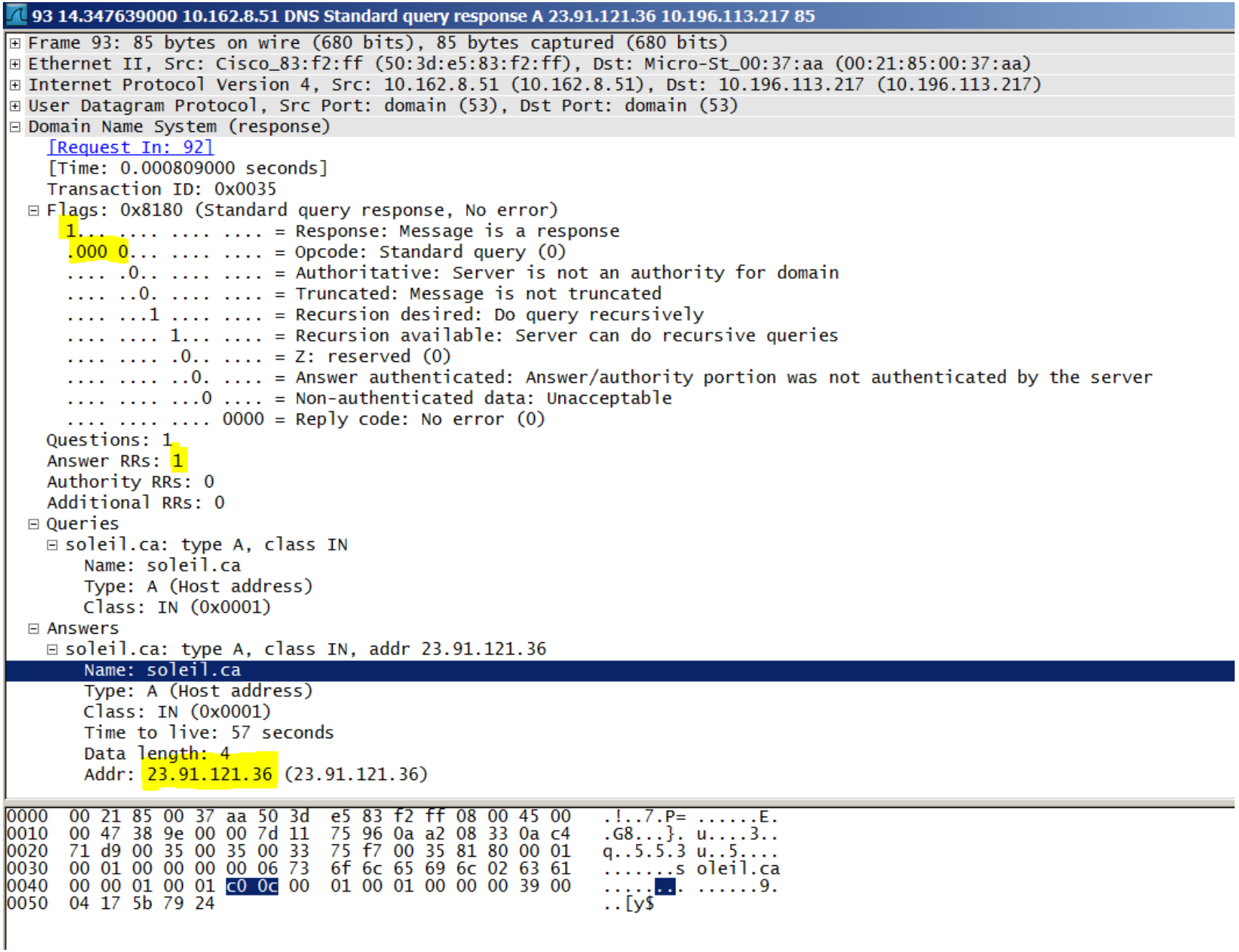


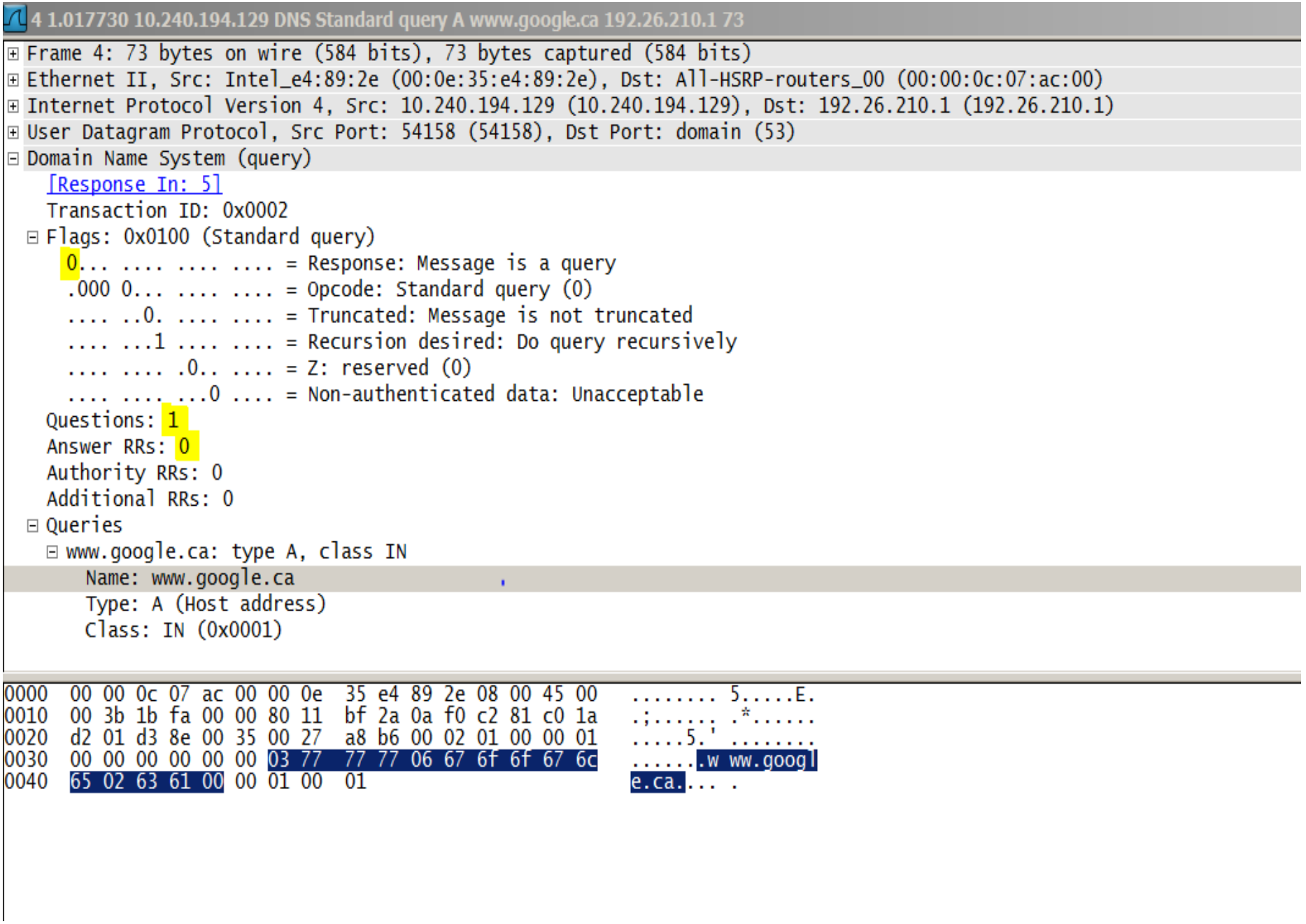
Champ Réponse (Answer)

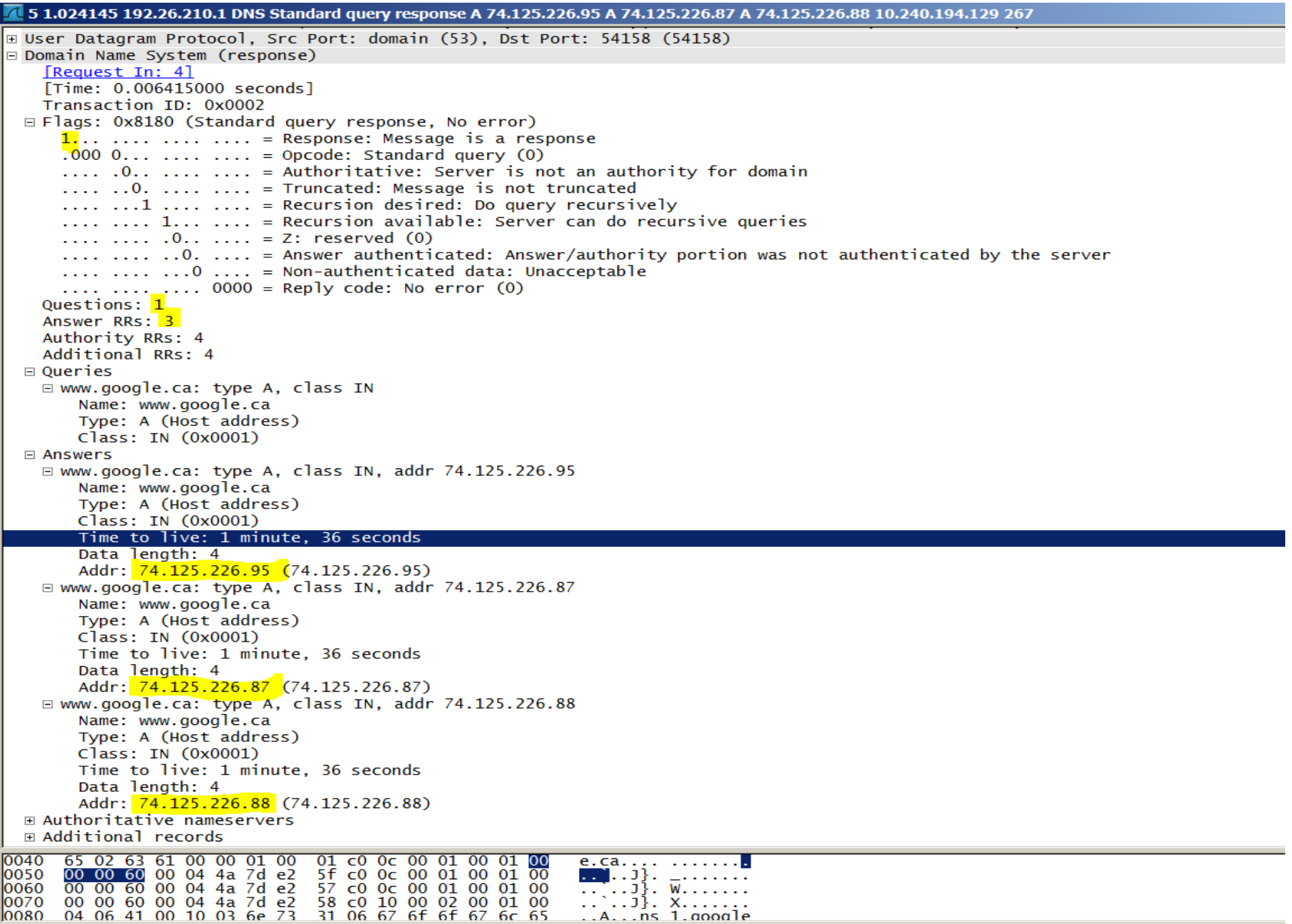
- NAME: Nom du domaine (offset)
- TYPE: type de réponses (RDATA).
- CLASS: type de protocole.
- TTL: durée de vie du résultat.
- RDLENGTH: longueur du champ RDATA.
- RDATA: les réponses retournées par le serveur contacté. Le format de ce champ dépend du champ TYPE. (si A records alors la longueur est 4 octets)




92 14.346830000 10.196.113.217 DNS Standard query A soleil.ca 10.162.8.51 69
Frame 92: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)
Ethernet II, Src: Micro-St_00:37:aa (00:21:85:00:37:aa), Dst: Cisco_83:f2:ff (50:3d:e5:83:f2:ff)
Internet Protocol Version 4, Src: 10.196.113.217 (10.196.113.217), Dst: 10.162.8.51 (10.162.8.51)
User Datagram Protocol, Src Port: domain (53), Dst Port: domain (53)
Source port: domain (53)
Destination port: domain (53)
Length: 35
Checksum: 0xc1e9 [validation disabled]
Domain Name System (query)
[Response In: 93]
Transaction ID: 0x0035
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
Queries
soleil.ca: type A, class IN
Name: soleil.ca
Type: A (Host address)
Class: IN (0x0001)
0000 50 3d e5 83 f2 ff 00 21 85 00 37 aa 08 00 45 00 P=.....! ..7...E.
0010 00 37 62 c0 00 00 80 11 48 84 0a c4 71 d9 0a a2 .7b..... H...q...
0020 08 33 00 35 00 35 00 23 c1 e9 00 35 01 00 00 01 .3.5.5.# ...5....
0030 00 00 00 00 00 00 06 73 6f 6c 65 69 6c 02 63 61 .....s oleil.ca
0040 00 00 01 00 01 .....


93 14.347639000 10.162.8.51 DNS Standard query response A 23.91.121.36 10.196.113.217 85
Frame 93: 85 bytes on wire (680 bits), 85 bytes captured (680 bits)
Ethernet II, Src: Cisco_83:f2:ff (50:3d:e5:83:f2:ff), Dst: Micro-St_00:37:aa (00:21:85:00:37:aa)
Internet Protocol Version 4, Src: 10.162.8.51 (10.162.8.51), Dst: 10.196.113.217 (10.196.113.217)
User Datagram Protocol, Src Port: domain (53), Dst Port: domain (53)
Domain Name System (response)
[Request In: 92]
[Time: 0.000809000 seconds]
Transaction ID: 0x0035
Flags: 0x8180 (Standard query response, No error)
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative: Server is not 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
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
soleil.ca: type A, class IN
Name: soleil.ca
Type: A (Host address)
Class: IN (0x0001)
Answers
soleil.ca: type A, class IN, addr 23.91.121.36
Name: soleil.ca
Type: A (Host address)
Class: IN (0x0001)
Time to live: 57 seconds
Data length: 4
Addr: 23.91.121.36 (23.91.121.36)
0000 00 21 85 00 37 aa 50 3d e5 83 f2 ff 08 00 45 00 .!..7.P= ......E.
0010 00 47 38 9e 00 00 7d 11 75 96 0a a2 08 33 0a c4 .G8...}. u....3..
0020 71 d9 00 35 00 35 00 33 75 f7 00 35 81 80 00 01 q..5.5.3 u..5....
0030 00 01 00 00 00 00 06 73 6f 6c 65 69 6c 02 63 61 ....s oleil.ca
0040 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00 39 00 ....9.
0050 04 17 5b 79 24 ..[y$


4 1.017730 10.240.194.129 DNS Standard query A www.google.ca 192.26.210.1 73
Frame 4: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
Ethernet II, Src: Intel_e4:89:2e (00:0e:35:e4:89:2e), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
Internet Protocol Version 4, Src: 10.240.194.129 (10.240.194.129), Dst: 192.26.210.1 (192.26.210.1)
User Datagram Protocol, Src Port: 54158 (54158), Dst Port: domain (53)
Domain Name System (query)
[Response In: 5]
Transaction ID: 0x0002
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
Queries
www.google.ca: type A, class IN
Name: www.google.ca
Type: A (Host address)
Class: IN (0x0001)
0000 00 00 0c 07 ac 00 00 0e 35 e4 89 2e 08 00 45 00 .... 5.....E.
0010 00 3b 1b fa 00 00 80 11 bf 2a 0a f0 c2 81 c0 1a .;..... .*......
0020 d2 01 d3 8e 00 35 00 27 a8 b6 00 02 01 00 00 01 .....5.' ....
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c ....w ww.googl
0040 65 02 63 61 00 00 01 00 01 e.ca.... .


5 1.024145 192.26.210.1 DNS Standard query response A 74.125.226.95 A 74.125.226.87 A 74.125.226.88 10.240.194.129 267
User Datagram Protocol, Src Port: domain (53), Dst Port: 54158 (54158)
Domain Name System (response)
[Request In: 4]
[Time: 0.006415000 seconds]
Transaction ID: 0x0002
Flags: 0x8180 (Standard query response, No error)
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative: Server is not 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
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 3
Authority RRs: 4
Additional RRs: 4
Queries
www.google.ca: type A, class IN
Name: www.google.ca
Type: A (Host address)
Class: IN (0x0001)
Answers
www.google.ca: type A, class IN, addr 74.125.226.95
Name: www.google.ca
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 minute, 36 seconds
Data length: 4
Addr: 74.125.226.95 (74.125.226.95)
www.google.ca: type A, class IN, addr 74.125.226.87
Name: www.google.ca
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 minute, 36 seconds
Data length: 4
Addr: 74.125.226.87 (74.125.226.87)
www.google.ca: type A, class IN, addr 74.125.226.88
Name: www.google.ca
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 minute, 36 seconds
Data length: 4
Addr: 74.125.226.88 (74.125.226.88)
Authoritative nameservers
Additional records
0040 65 02 63 61 00 00 01 00 01 c0 0c 00 01 00 01 00 e.ca.... ....
0050 00 00 60 00 04 4a 7d e2 5f c0 0c 00 01 00 01 00 ..`..J}. _.......
0060 00 00 60 00 04 4a 7d e2 57 c0 0c 00 01 00 01 00 ..`..J}. W.......
0070 00 00 60 00 04 4a 7d e2 58 c0 10 00 02 00 01 00 ..`..J}. X.......
0080 04 06 41 00 10 03 6e 73 31 06 67 6f 6f 67 6c 65 ..A...ns 1.google