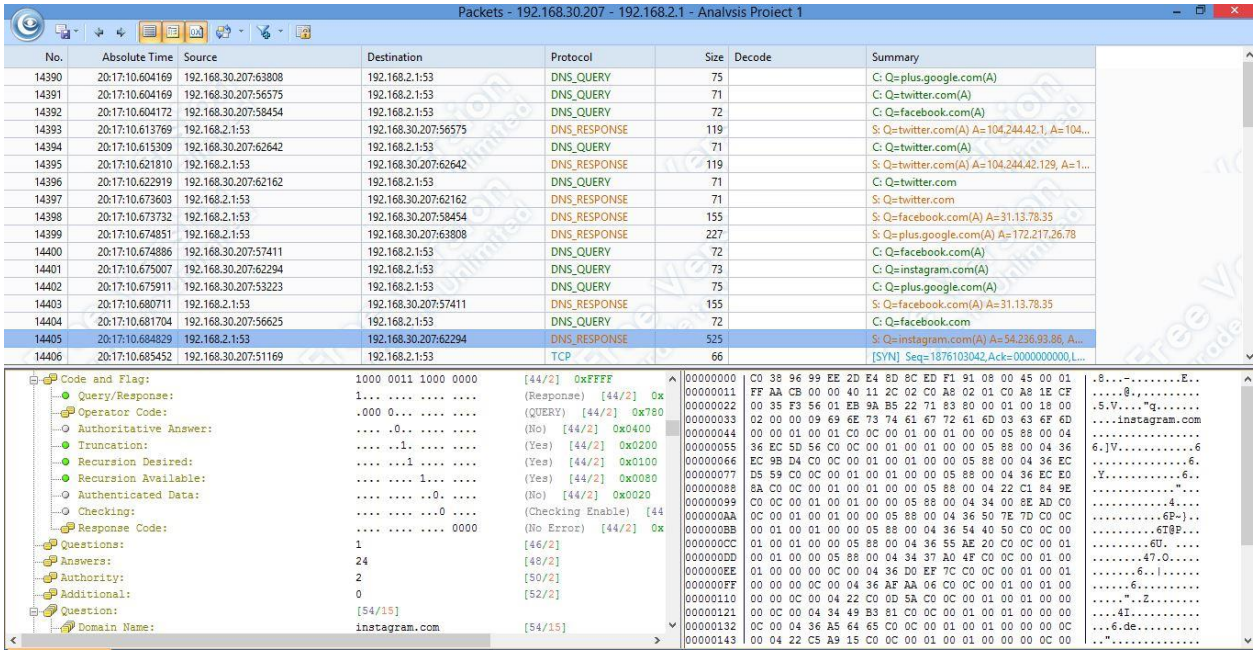
Analisis Menggunakan Colasoft Capsa

Nama : Dera Cahyani
NIM : 09031181520004
Kelas : SIREG 4B

Sistem Informasi
Fakultas Ilmu Komputer
Universitas Sriwijaya

Disini saya menganalisis menggunakan colasoft capsa 9 free. Saya menggunakan packets IP 192.168.30.207 ini adalah IP source kita – 192.168.2.1. dan ini adalah IP destination kita.

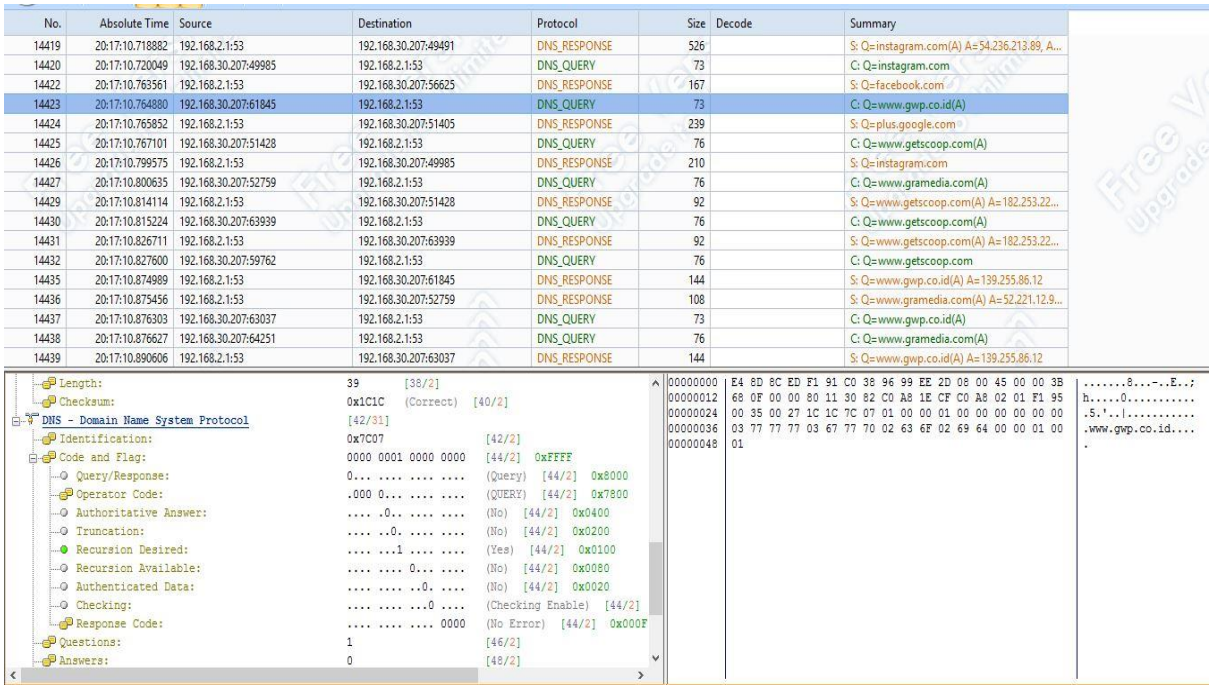


Terlihat pada gambar diatas banyak sekali yang dapat kita akses menggunakan IP ini. Pada baris pertama terlihat bahwa IP source kita mengakses ke IP destination yang kita tuju dengan size panjang paketnya yaitu 75 untuk dapat mengakses ke plus.google.com. pada baris kedua merupakan IP source yang mengakses IP destination twitter.com dengan panjang paketnya yaitu 71. Pada baris ketiga IP sorce juga dapat mengakses facebook.com dengan nomor IP destination yang sama tetapi dengan panjang paket yang berbeda yaitu 72.

Baris selanjutnya merupakan DNS Response dari IP destination yang kita tuju yaitu dari twitter.com dengan panjang paketnya yaitu 119.pada nomor 14401 kita mendapatkan IP destination yang baru yaitu ke alamat instagram.com dengan IP destination yang sama dengan sebelumnya dan mempunyai panjang paket sebanyak 73.

Dari gambar diatas ternyata alamat IP source tersebut dapat mengakses banyak halaman. Pada nomor 14423 IP tersebut dapat mengakses alamat website www.gwp.co.id dengan panjang paketnya 73. Selanjutnya pada nomor 14425 IP sorce tersebut juga dapat mengakses www.getscoop.com dengan panjang paketnya 76. Dan pada nomor 14427 IP source tersebut juga dapat melakukan pengaksesan dengan destination www.gramedia.com. IP source ini juga dapat mengakses dengan IP destination yang sama tetapi dengan alamat yang berbeda yaitu www.linkedin.com dengan panjang paketnya sebanyak 72. Selanjutnya IP

sorce tersebut dapat mengakses website tumblr.com dengan panjang paketnya sebanyak 70. Selanjutnya IP source ini dapat mengakses t.co dengan panjang paketnya sebanyak 60.



No.	Absolute Time	Source	Destination	Protocol	Size	Decode	Summary
14419	20:17:10.718882	192.168.2.1:53	192.168.30.207:49491	DNS_RESPONSE	526		S: Q=instagram.com(A) A=54.236.213.89, A...
14420	20:17:10.720049	192.168.30.207:49985	192.168.2.1:53	DNS_QUERY	73		C: Q=instagram.com
14422	20:17:10.763561	192.168.2.1:53	192.168.30.207:56625	DNS_RESPONSE	167		S: Q=facebook.com
14423	20:17:10.764880	192.168.30.207:61845	192.168.2.1:53	DNS_QUERY	73		C: Q=www.gwp.co.id(A)
14424	20:17:10.765852	192.168.2.1:53	192.168.30.207:51405	DNS_RESPONSE	239		S: Q=plus.google.com
14425	20:17:10.767101	192.168.30.207:51428	192.168.2.1:53	DNS_QUERY	76		C: Q=www.getscoop.com(A)
14426	20:17:10.799575	192.168.2.1:53	192.168.30.207:49985	DNS_RESPONSE	210		S: Q=instagram.com
14427	20:17:10.800635	192.168.30.207:52759	192.168.2.1:53	DNS_QUERY	76		C: Q=www.gramedia.com(A)
14429	20:17:10.814114	192.168.2.1:53	192.168.30.207:51428	DNS_RESPONSE	92		S: Q=www.getscoop.com(A) A=182.253.22...
14430	20:17:10.815224	192.168.30.207:63939	192.168.2.1:53	DNS_QUERY	76		C: Q=www.getscoop.com(A)
14431	20:17:10.826711	192.168.2.1:53	192.168.30.207:63939	DNS_RESPONSE	92		S: Q=www.getscoop.com(A) A=182.253.22...
14432	20:17:10.827600	192.168.30.207:59762	192.168.2.1:53	DNS_QUERY	76		C: Q=www.getscoop.com
14435	20:17:10.874989	192.168.2.1:53	192.168.30.207:61845	DNS_RESPONSE	144		S: Q=www.gwp.co.id(A) A=139.255.86.12
14436	20:17:10.875456	192.168.2.1:53	192.168.30.207:52759	DNS_RESPONSE	108		S: Q=www.gramedia.com(A) A=52.221.12.9...
14437	20:17:10.876303	192.168.30.207:63037	192.168.2.1:53	DNS_QUERY	73		C: Q=www.gwp.co.id(A)
14438	20:17:10.876627	192.168.30.207:64251	192.168.2.1:53	DNS_QUERY	76		C: Q=www.gramedia.com(A)
14439	20:17:10.890606	192.168.2.1:53	192.168.30.207:63037	DNS_RESPONSE	144		S: Q=www.gwp.co.id(A) A=139.255.86.12

```
Length:                    39          [38/2]
Checksum:                  0x1C1C      (Correct)  [40/2]
DNS - Domain Name System Protocol      [42/31]
  Identification:          0x7C07                 [42/2]
  Code and Flag:           0000 0001 0000 0000    [44/2]  0xFFFF
    Query/Response:        0... .... .... ....    (Query)  [44/2]  0x8000
    Operator Code:         .000 0... .... ....    (QUERY)  [44/2]  0x7800
    Authoritative Answer:  .... .0.. .... ....    (No)  [44/2]  0x0400
    Truncation:            .... ..0. .... ....    (No)  [44/2]  0x0200
    Recursion Desired:     .... ...1 .... ....    (Yes)  [44/2]  0x0100
    Recursion Available:   .... .... 0... ....    (No)  [44/2]  0x0080
    Authenticated Data:    .... .... ..0. ....    (No)  [44/2]  0x0020
    Checking:              .... .... ...0 ....    (Checking Enable)  [44/2]
    Response Code:         .... .... .... 0000    (No Error)  [44/2]  0x000F
  Questions:               1                      [46/2]
  Answers:                 0                      [48/2]
```

```
00000000  E4 8D 8C ED F1 91 C0 38 96 99 EE 2D 08 00 45 00 00 3B  .......8...-..E..;
00000012  68 0F 00 00 80 11 30 82 C0 A8 1E CF C0 A8 02 01 F1 95  h.....0.........
00000024  00 35 00 27 1C 1C 7C 07 01 00 00 01 00 00 00 00 00 00  .5.'..|.........
00000036  03 77 77 77 03 67 77 70 02 63 6F 02 69 64 00 00 01 00  .www.gwp.co.id....
00000048  01                                                      .
```

Jadi, menurut hasil analisis saya diatas. Satu IP source dapat mengakses banyak website dengan IP Destination yang sama. Dan juga dengan Packet Length yang berbeda-beda sesuai dengan jarak ataupun traffic yang kita tuju. Terdapat juga DNS Query dan DNS Response. DNS query merupakan system database yang kita pinta untuk menuju ke alamat yang kita tuju. Sedangkan DNS Response merupakan system database dari server ke client. Panjang paket berbeda antara DNS query dengan DNS Response Karena banyak traffic antara saat server memberikan data kepada kita dari saat kita meminta data kepada server.

Sekian analisis ini saya buat, bila ada salah mohon dimaafkan dan dikoreksi. Terimakasih.