

KOMUNIKASI DATA DAN JARINGAN KOMPUTER

TUGAS 2



DISUSUN OLEH

NAMA : SELLY INDRIYANI
NIM : 09031181520116
KELAS : SI REG 4B
DOSEN PENGAMPUH : DERIS STIAWAN, PH.D

**FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM INFORMASI
UNIVERSITAS SRIWIJAYA
2017**

MENGANALISA TRAFIC PADA IP CONVERSATION DAN MATRIX

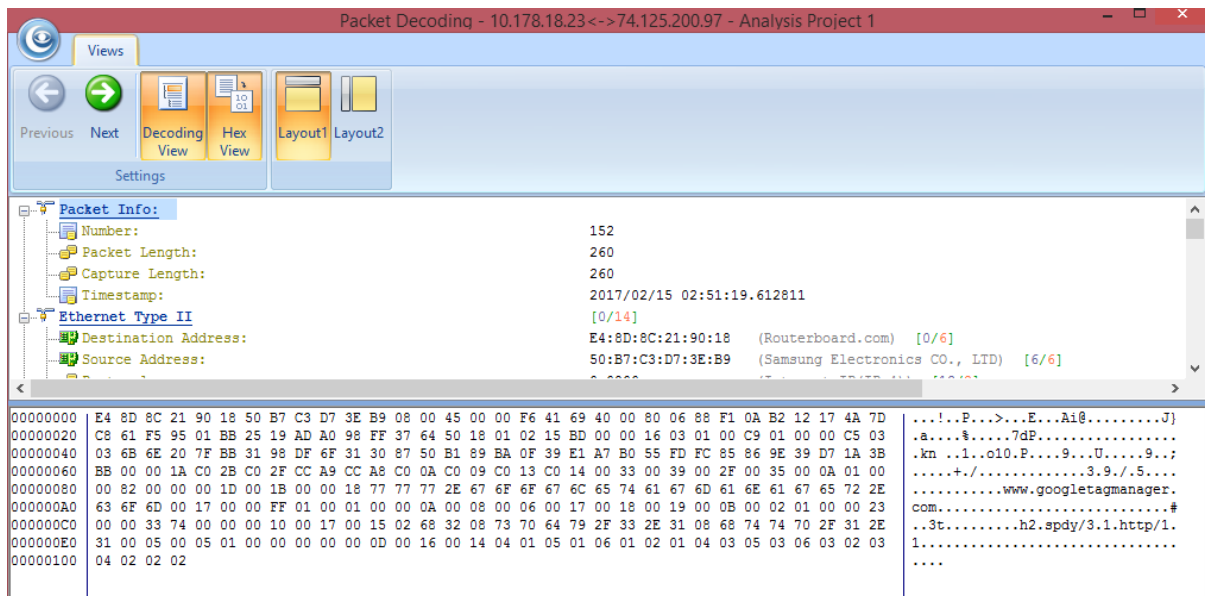
Untuk membandingkan Traffic pada IP Conversation dan Matrix kita terlebih dahulu mencari traffic dari client ke destination pada Wireshark dalam hal ini saya menggunakan web server Indonesia yaitu Telkomsel.com.

IP Conversation

IP Conversation merupakan percakapan yang menunjukkan statistik komunikasi jaringan antara dua alamat IP.

Berikut adalah 10 IP Address yang saya analisis berdasarkan destination www.telkomsel.com :

1. 10.178.18.23 <-> 74.125.200.97



Hasil Analisis :

Berdasarkan tampilan diatas hasil komunikasi antara IP Address 10.178.18.23 dengan IP Address 74.125.200.97 menunjukkan bahwa sedang mengakses alamat web www.googletagmanager.com

2. 74.125.200.97 <-> 10.178.18.23

The screenshot shows a Wireshark packet capture window titled "Packet Decoding - 74.125.200.97 <-> 10.178.18.23 - Analysis Project 1". The interface includes navigation buttons (Previous, Next, Decoding View, Hex View, Layout1, Layout2) and a "Settings" section. The "Packet Info" pane displays the following details:

- Number: 162
- Packet Length: 902
- Capture Length: 902
- Timestamp: 2017/02/15 02:51:19.659772
- Ethernet Type II: [0/14]
- Destination Address: 50:B7:C3:D7:3E:B9 (Samsung Electronics CO., LTD) [0/6]
- Source Address: E4:8D:8C:21:90:18 (Routerboard.com) [6/6]
- Protocol: 0x0800 (Internet IP(IPv4)) [12/2]

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII portion of the packet is an HTTP GET request:

```
h.+...G.#.03...0...U.....z
.h.....d.})e...N0...U.....0
...0...U.....0:..U...301
0/..-+.)http://crl.geotrust.com
/crl/secureca.crl0N..U..G0E0C
..U..0;09..+.....-https://w
ww.geotrust.com/resources/repos
itory0...*.H.....v..nNK.
..0.....q-f.....N.C8..
0)..U..j.6...Hf.m...G..2\s....
```

Hasil Analisis :

Berdasarkan tampilan diatas hasil komunikasi antara IP Address 74.125.200.97 dengan IP Address 10.178.18.23 menunjukkan bahwa sedang mengakses alamat web www.geotrust.com

3. 103.241.4.11 <-> 10.178.18.23

The screenshot shows a Wireshark packet capture window titled "Packet Decoding - 103.241.4.11 <-> 10.178.18.23 - Analysis Project 1". The interface includes navigation buttons (Previous, Next, Decoding View, Hex View, Layout1, Layout2) and a "Settings" section. The "Packet Info" pane displays the following details:

- Number: 1,457
- Packet Length: 283
- Capture Length: 283
- Timestamp: 2017/02/15 02:51:55.490514
- Ethernet Type II: [0/14]
- Destination Address: 50:B7:C3:D7:3E:B9 (Samsung Electronics CO., LTD) [0/6]
- Source Address: E4:8D:8C:21:90:18 (Routerboard.com) [6/6]

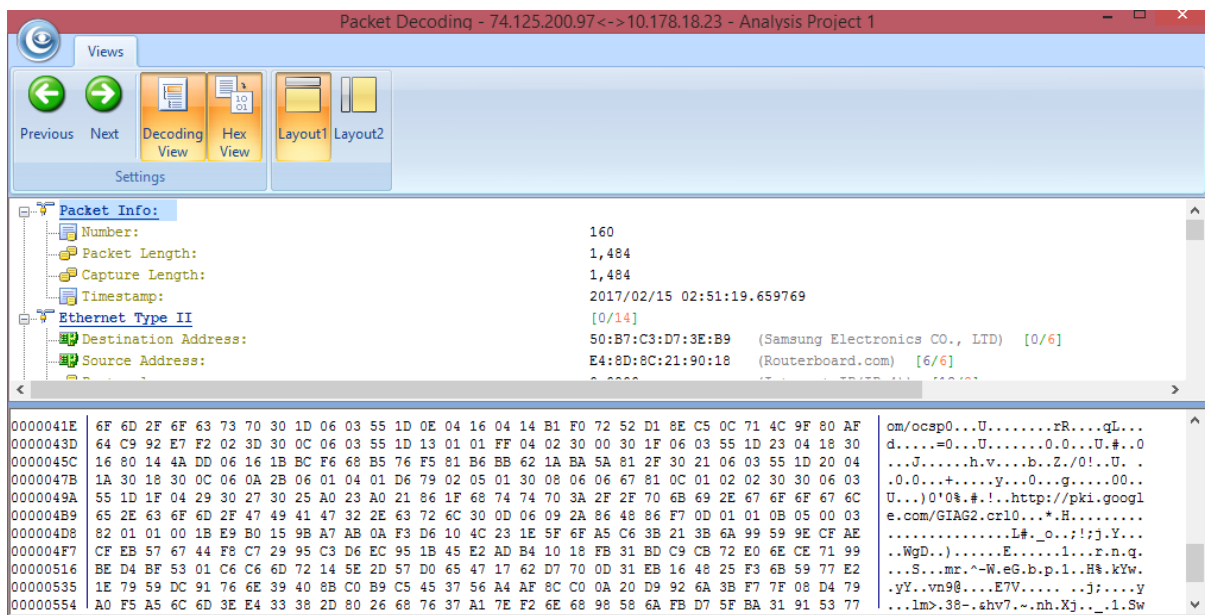
The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII portion of the packet is an HTTP GET request:

```
P...>...!...E...T...@...g....
...5.....6.....*pipeline-
tee-n-elb-1f4e4sjxqtxp-28517224
6.us-west-2.elb.amazonaws.com...
...7.....ns-1769.awsdns-29
.co.uk..7.....ns-332.awsdn
s-41.0.7.....ns-560.awsdns
-06.net..7.....ns-1475.aws
dns-56.org.....-.....L
```

Hasil Analisis :

Berdasarkan tampilan diatas hasil komunikasi antara IP Address 103.241.4.11 dengan IP Address 10.178.18.23 menunjukkan bahwa sedang mengakses alamat web www.amazonaws.com

4. 74.125.200.97 <-> 10.178.18.23



Packet Decoding - 74.125.200.97<->10.178.18.23 - Analysis Project 1

Views: Previous, Next, Decoding View, Hex View, Layout1, Layout2

Packet Info:

- Number: 160
- Packet Length: 1,484
- Capture Length: 1,484
- Timestamp: 2017/02/15 02:51:19.659769
- Ethernet Type II
 - Destination Address: 50:B7:C3:D7:3E:B9 (Samsung Electronics CO., LTD) [0/6]
 - Source Address: E4:8D:8C:21:90:18 (Routerboard.com) [6/6]

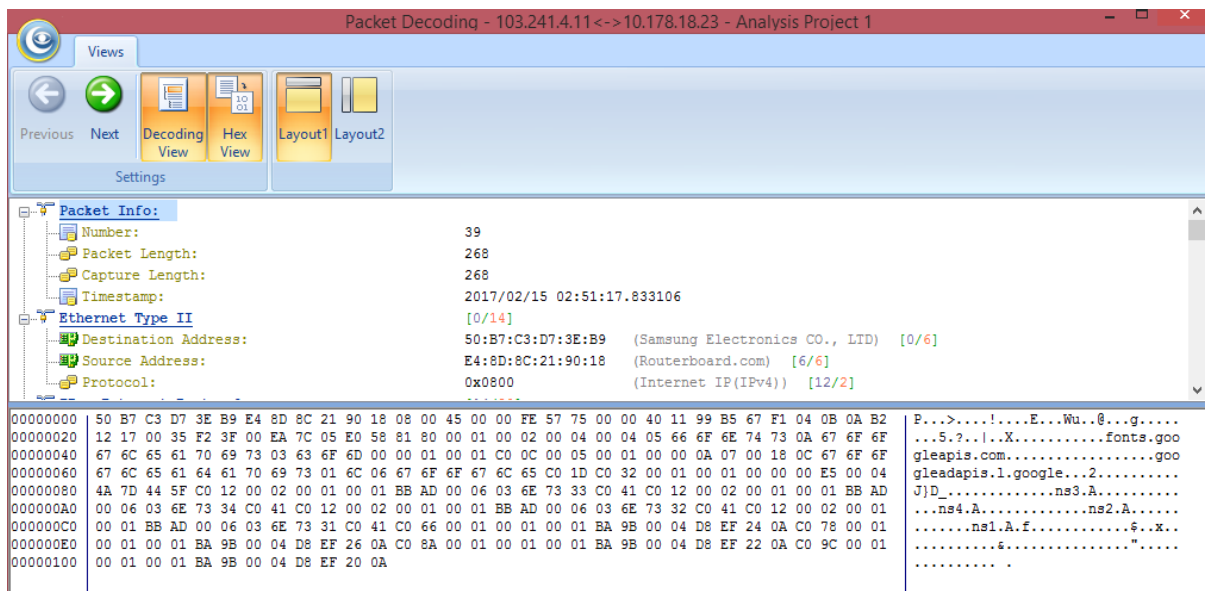
Raw packet bytes (hex and ASCII):

```
0000041E 6F 6D 2F 6F 63 73 70 30 1D 06 03 55 1D 0E 04 16 04 14 B1 F0 72 52 D1 8E C5 0C 71 4C 9F 80 AF om/ocsp0...U.....r...qL...
0000043D 64 C9 92 E7 F2 02 3D 30 0C 06 03 55 1D 13 01 01 FF 04 02 30 00 30 1F 06 03 55 1D 23 04 18 30 d.....=0...U...0.0...U.#..0
0000045C 16 80 14 4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 BB 62 1A BA 5A 81 2F 30 21 06 03 55 1D 20 04 ...J...h.v...b.Z/0!..U...
0000047B 1A 30 18 30 0C 06 0A 2B 06 01 04 01 D6 79 02 05 01 30 08 06 06 67 81 0C 01 02 02 30 30 06 03 .0.0...+...y..0..g...00..
0000049A 55 1D 1F 04 29 30 27 30 25 A0 23 A0 21 86 1F 68 74 74 70 3A 2F 2F 70 6B 69 2E 67 6F 6F 67 6C U...}0'0$.#!..http://pki.googl
000004B9 65 2E 63 6F 6D 2F 47 49 41 47 32 2E 63 72 6C 30 0D 06 09 2A 86 48 86 F7 0D 01 01 0B 05 00 03 e.com/GIAG2.crl0...*.H...
000004D8 82 01 01 00 1B E9 B0 15 9B A7 AB 0A F3 D6 10 4C 23 1E 5F 6F A5 C6 3B 21 3B 6A 99 59 9E CF AE .....L#.o...!;j.Y...
000004F7 CF EB 57 67 44 F8 C7 29 95 C3 D6 EC 95 1B 45 E2 AD B4 10 18 FB 31 BD C9 CB 72 E0 6E CE 71 99 ..WgD...).....E...1...r.n.g...
00000516 BE D4 BF 53 01 C6 C6 6D 72 14 5E 2D 57 D0 65 47 17 62 D7 70 0D 31 EB 16 48 25 F3 6B 59 77 E2 ...S...mr.^-W.eG.b.p.l.H%.kYw...
00000535 1E 79 59 DC 91 76 6E 39 40 8B C0 B9 C5 45 37 56 A4 AF 8C C0 0A 20 D9 92 6A 3B F7 7F 08 D4 79 .yY.vn9@...E7V... ..j;...y
00000554 A0 F5 A5 6C 6D 3E E4 33 38 2D 80 26 68 76 37 A1 7E F2 6E 68 98 58 6A FB D7 5F BA 31 91 53 77 ...lm>.38-.zhv7.-.nh.Xj..._1.Sw
```

Hasil Analisis :

Berdasarkan tampilan diatas hasil komunikasi antara IP Address 74.125.200.97 dengan IP Address 10.178.18.23 menunjukkan bahwa sedang mengakses alamat web www.pki.google.com

5. 103.241.4.11 <-> 10.178.18.23



Packet Decoding - 103.241.4.11<->10.178.18.23 - Analysis Project 1

Views: Previous, Next, Decoding View, Hex View, Layout1, Layout2

Packet Info:

- Number: 39
- Packet Length: 268
- Capture Length: 268
- Timestamp: 2017/02/15 02:51:17.833106
- Ethernet Type II
 - Destination Address: 50:B7:C3:D7:3E:B9 (Samsung Electronics CO., LTD) [0/6]
 - Source Address: E4:8D:8C:21:90:18 (Routerboard.com) [6/6]
 - Protocol: 0x0800 (Internet IP(IPv4)) [12/2]

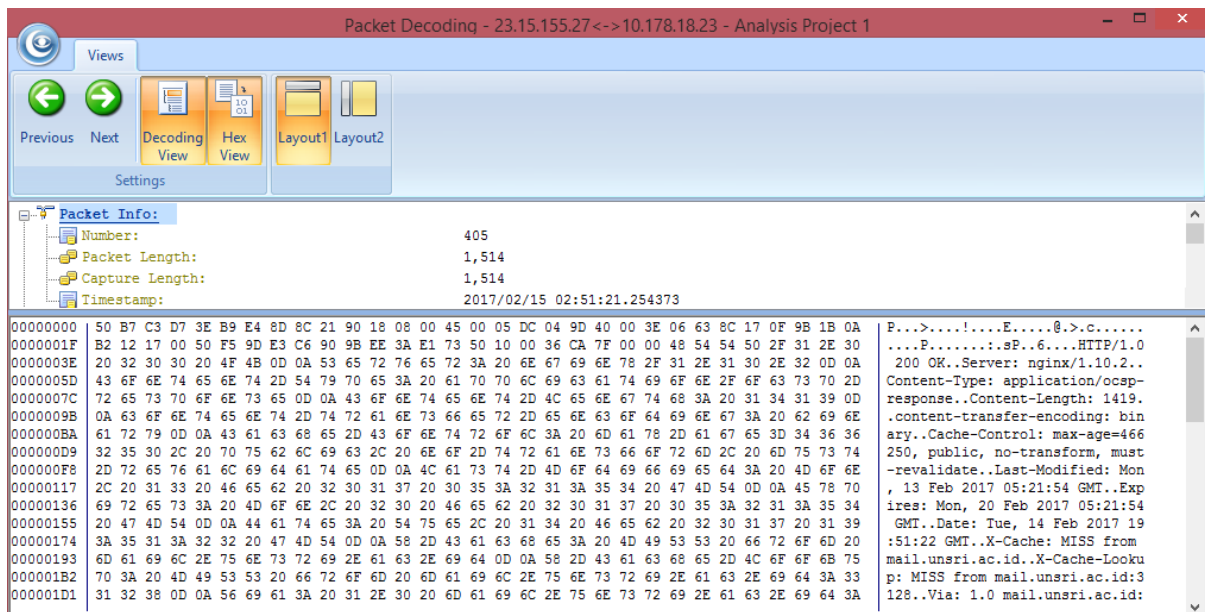
Raw packet bytes (hex and ASCII):

```
00000000 50 B7 C3 D7 3E B9 E4 8D 8C 21 90 18 08 00 45 00 00 FE 57 75 00 00 40 11 99 B5 67 F1 04 0B 0A B2 P...>...!...E...Wu..@...g....
00000020 12 17 00 35 F2 3F 00 EA 7C 05 E0 58 81 80 00 01 00 02 00 04 00 04 05 66 6F 6E 74 73 0A 67 6F 6F ...S?...!..X...fonts.goo
00000040 67 6C 65 61 70 69 73 03 63 6F 6D 00 00 01 00 01 C0 0C 00 05 00 01 00 00 0A 07 00 18 0C 67 6F 6F gleapis.com...google...goo
00000060 67 6C 65 61 64 61 70 69 73 01 6C 06 67 6F 6F 67 6C 65 C0 1D C0 32 00 01 00 01 00 00 00 E5 00 04 gleadapis.l.google...2...
00000080 4A 7D 44 5F C0 12 00 02 00 01 00 01 BB AD 00 06 03 6E 73 33 C0 41 C0 12 00 02 00 01 00 01 BB AD UJD_...ns3.A...
000000A0 00 06 03 6E 73 34 C0 41 C0 12 00 02 00 01 00 01 BB AD 00 06 03 6E 73 32 C0 41 C0 12 00 02 00 01 ..ns4.A... ..ns2.A...
000000C0 00 01 BB AD 00 06 03 6E 73 31 C0 41 C0 66 00 01 00 01 00 01 BA 9B 00 04 D8 EF 24 0A C0 78 00 01 ..ns1.A.f... ..s..x...
000000E0 00 01 00 01 BA 9B 00 04 D8 EF 26 0A C0 8A 00 01 00 01 00 01 BA 9B 00 04 D8 EF 22 0A C0 9C 00 01 .....&.....
00000100 00 01 00 01 BA 9B 00 04 D8 EF 20 0A
```

Hasil Analisis :

Berdasarkan tampilan diatas hasil komunikasi antara IP Address 103.241.4.11 dengan IP Address 10.178.18.23 menunjukkan bahwa sedang mengakses alamat web www.fonts.googleapis.com

6. 23.15.155.27 <-> 10.178.18.23



The screenshot shows a Wireshark packet capture analysis. The title bar reads "Packet Decoding - 23.15.155.27 <-> 10.178.18.23 - Analysis Project 1". The interface includes navigation buttons (Previous, Next, Decoding View, Hex View, Layout1, Layout2) and a "Settings" section. The "Packet Info" pane shows:

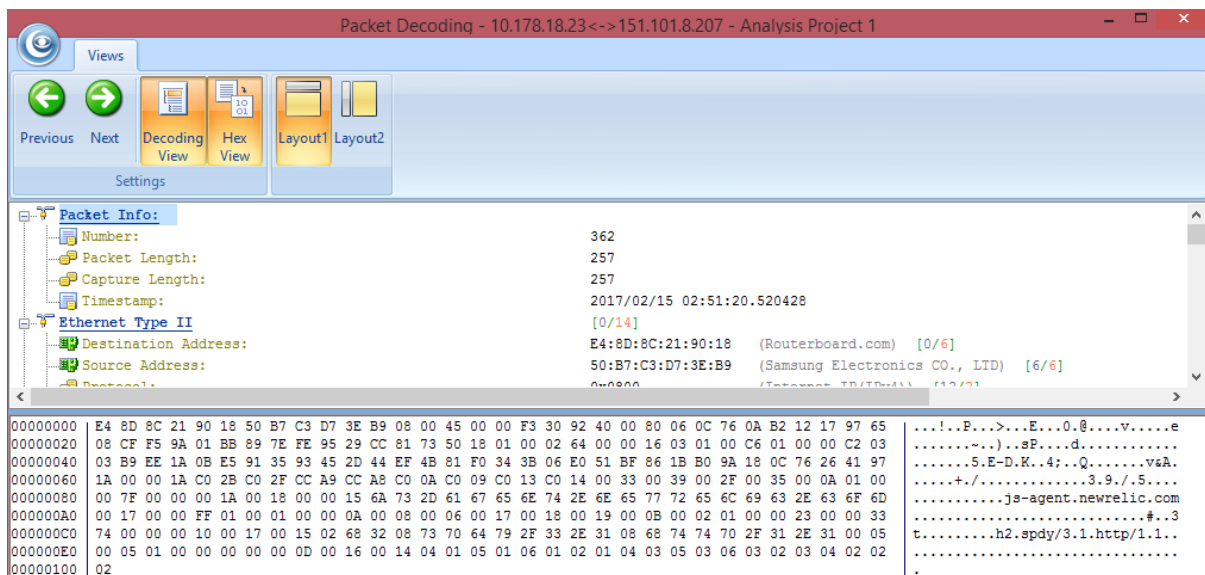
- Number: 405
- Packet Length: 1,514
- Capture Length: 1,514
- Timestamp: 2017/02/15 02:51:21.254373

The packet list pane shows a single entry for packet 405. The packet bytes pane displays the raw data in hexadecimal and ASCII. The ASCII portion shows an HTTP 200 OK response from a server with headers including "Server: nginx/1.10.2..", "Content-Type: application/octet-stream", and "Cache-Control: max-age=466250, public, no-transform, must-revalidate..Last-Modified: Mon, 13 Feb 2017 05:21:54 GMT..Expires: Mon, 20 Feb 2017 05:21:54 GMT..Date: Tue, 14 Feb 2017 19:51:22 GMT..X-Cache: MISS from mail.unsri.ac.id..X-Cache-Lookup: MISS from mail.unsri.ac.id:3128..Via: 1.0 mail.unsri.ac.id:".

Hasil Analisis :

Berdasarkan tampilan diatas hasil komunikasi antara IP Address 23.15.155.27 dengan IP Address 10.178.18.23 menunjukkan bahwa sedang mengakses alamat web www.mail.unsri.ac.id

7. 10.178.18.23 <-> 151.101.8.207



The screenshot shows a Wireshark packet capture analysis. The title bar reads "Packet Decoding - 10.178.18.23 <-> 151.101.8.207 - Analysis Project 1". The interface includes navigation buttons (Previous, Next, Decoding View, Hex View, Layout1, Layout2) and a "Settings" section. The "Packet Info" pane shows:

- Number: 362
- Packet Length: 257
- Capture Length: 257
- Timestamp: 2017/02/15 02:51:20.520428

The "Ethernet Type II" pane shows:

- Destination Address: E4:8D:8C:21:90:18 (Routerboard.com) [0/6]
- Source Address: 50:B7:C3:D7:3E:B9 (Samsung Electronics CO., LTD) [6/6]

The packet bytes pane displays the raw data in hexadecimal and ASCII. The ASCII portion shows a JavaScript snippet starting with "P...>...E...0@...v...e...P...d...S-E-D.K..4:..Q...v&A...+./...3.9./...js-agent.newrelic.com...#..3...h2.spdy/3.1.http/1.1..."

Hasil Analisis :

Berdasarkan tampilan diatas hasil komunikasi antara IP Address 10.178.18.23 dengan IP Address 151.101.8.207 menunjukkan bahwa sedang mengakses alamat web www.newrelic.com

8. 10.178.18.23 <-> 52.43.25.167

Packet Decoding - 10.178.18.23<->52.43.25.167 - Analysis Project 1

Views: Previous, Next, Decoding View, Hex View, Layout1, Layout2

Settings

Packet Info:

- Number: 1,461
- Packet Length: 266
- Capture Length: 266
- Timestamp: 2017/02/15 02:51:55.491911

Ethernet II

- Destination Address: E4:8D:8C:21:90:18 (Routerboard.com) [0/6]
- Source Address: 50:B7:C3:D7:3E:B9 (Samsung Electronics CO., LTD) [6/6]

00000000 E4 8D 8C 21 90 18 50 B7 C3 D7 3E B9 08 00 45 00 00 FC 3C 7A 40 00 80 06 52 E7 0A B2 12 17 34 2BP...>...E...<z@...R....4+

00000020 19 A7 F5 B6 01 BB 56 A2 F0 EA 22 3D A5 76 50 18 FA F0 7F 75 00 00 16 03 01 00 CF 01 00 00 CB 03V...".vP...u.....

00000040 03 CA 09 DD BC B3 51 D9 ED 55 29 05 88 17 BB 68 ED 1F 2B 11 8E 7C CB FB F7 96 CE BF FF 06 86 66Q..U)...h..+...|.....f

00000060 F2 00 00 1A C0 2B C0 2F CC A9 CC A8 C0 0A C0 09 C0 13 C0 14 00 33 00 39 00 2F 00 35 00 0A 01 00+./...incoming.telemetry.mo

00000080 00 88 00 00 23 00 21 00 00 1E 69 6E 63 6F 6D 69 6E 67 2E 74 65 6C 65 6D 65 74 72 79 2E 6D 6F#.!....zilla.org

000000A0 7A 69 6C 6C 61 2E 6F 72 67 00 17 00 00 FF 01 00 01 00 00 0A 00 08 00 06 00 17 00 18 00 19 00 0B#.!.3t.....h2.spdy/3.1.h

000000C0 00 02 01 00 00 23 00 00 33 74 00 00 10 00 17 00 15 02 68 32 08 73 70 64 79 2F 33 2E 31 08 68#.!.3t.....h2.spdy/3.1.h

000000E0 74 74 70 2F 31 2E 31 00 05 00 05 01 00 00 00 00 0D 00 16 00 14 04 01 05 01 06 01 02 01 04 03 ttp/1.1.....

00000100 05 03 06 03 02 03 04 02 02 02

Hasil Analisis :

Berdasarkan tampilan diatas hasil komunikasi antara IP Address 10.178.18.23 dengan IP Address 52.43.25.167 menunjukkan bahwa sedang mengakses alamat web www.mozilla.org

9. 151.101.8.207 <-> 10.178.18.23

Packet Decoding - 151.101.8.207<->10.178.18.23 - Analysis Project 1

Views: Previous, Next, Decoding View, Hex View, Layout1, Layout2

Settings

Packet Info:

- Packet Length: 1,514
- Capture Length: 1,514
- Timestamp: 2017/02/15 02:51:20.596999

Ethernet II

- Destination Address: 50:B7:C3:D7:3E:B9 (Samsung Electronics CO., LTD) [0/6]
- Source Address: E4:8D:8C:21:90:18 (Routerboard.com) [6/6]

Protocol: 0x0800 (Internet IP(IPv4)) [12/2]

000003A2 C4 45 AD 6E 2B 63 AB 92 6B 61 0A 4D 20 ED 73 BA 7C CE FE 16 B5 DB 9F 80 F0 D6 8B 6C D9 08 79 .E.n+C..ka.M.s.|.....1.y

000003C1 4A 4F 78 65 DA 92 BC BE 35 F9 B3 C4 F9 27 80 4E FF 96 52 E6 02 20 E1 07 73 E9 5D 2B BD B2 F1 J0xe...S...'.N.R...s.]+...

000003E0 02 03 01 00 01 A3 82 01 25 30 82 01 21 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02 01 06 30 12#0..!0..U.....0.

000003FF 06 03 55 1D 13 01 01 FF 04 08 30 06 01 01 FF 02 01 00 30 1D 06 03 55 1D 0E 04 16 04 14 96 DE ..U.....0.....0...U.....

0000041E 61 F1 BD 1C 16 29 53 1C C0 CC 7D 3B 83 00 40 E6 1A 7C 30 47 06 03 55 1D 20 04 40 30 3E 30 3C a...S...;].@..!0G..U..@0>0<

0000043D 06 04 55 1D 20 00 30 34 30 32 06 08 2B 06 01 05 05 07 30 01 86 21 68 74 74 70 3A 2F 2F 6F 77 ..U..0402..+.....&https://w

0000045C 77 77 2E 67 6C 6F 62 61 6C 73 69 67 6E 2E 63 6F 6D 2F 72 65 70 6F 73 69 74 6F 72 79 2F 30 33 ww.globalsign.com/repository/03

0000047B 06 03 55 1D 1F 04 2C 30 2A 30 28 A0 26 A0 24 86 22 68 74 74 70 3A 2F 2F 63 72 6C 2E 67 6C 6F ..U...0*0(.z.s."http://crl.glo

0000049A 62 61 6C 73 69 67 6E 2E 6E 65 74 2F 72 6F 6F 74 2E 63 72 6C 30 3D 06 08 2B 06 01 05 05 07 01 balsign.net/root.crl0=+.....

000004B9 01 04 31 30 2F 30 2D 06 08 2B 06 01 05 05 07 30 01 86 21 68 74 74 70 3A 2F 2F 6F 63 73 70 2E ..10/0-...+...0.!http://ocsp.

000004D8 67 6C 6F 62 61 6C 73 69 67 6E 2E 63 6F 6D 2F 72 6F 6F 74 72 71 30 1F 06 03 55 1D 23 04 18 30 globalsign.com/rootr10..U..#..0

000004F7 16 80 14 60 7B 66 1A 45 0D 97 CA 89 50 2F 7D 04 CD 34 A8 FF FC FD 4B 30 0D 06 09 2A 86 48 86 ...'[E...P/)...4...R0...*.H.

00000516 F7 0D 01 01 0B 05 00 03 82 01 01 00 06 CA 2A EE 5E BD AE 01 60 37 31 11 86 71 74 B6 46 49 C8 10F*^...`71..qt.FI..

00000535 16 FE 2F 62 23 17 AB 1F 87 F8 82 ED CA DF 0E 2C DF 64 75 8E 85 18 72 A7 8C 3A 8B C9 AC A5 77 ../b#.....,du..E...:..w

00000554 50 F7 EF 9E A4 E0 A0 8F 14 57 A3 2A 5F EC 7E 6D 10 E6 BA 8D B0 08 87 76 0E 4C B2 D9 51 BB 11 P.....W*...-m.....v.L..Q..

00000573 02 F2 5C DD 1C BD F3 55 96 0F D4 06 C0 FC E2 23 8A 24 70 D3 BB F0 79 1A A7 61 70 83 8A AF 06 ..\...U.....#..sp...y...ap....

00000592 C5 20 D8 A1 63 D0 6C AE 4F 32 D7 AE 7C 18 45 75 05 29 77 DF 42 40 64 64 86 BE 2A 76 09 31 6F ..c.l.O2..!.Eu.)w.B@dd.*v.lo

000005B1 1D 24 F4 99 D0 85 FE F2 21 08 F9 C6 F6 F1 D0 59 ED D6 56 3C 08 28 03 67 BA F0 F9 F1 90 16 47 \$......!.!.....Y.v.<.(g.....G

Hasil Analisis :

Berdasarkan tampilan diatas hasil komunikasi antara IP Address 151.101.8.207 dengan IP Address 10.178.18.23 menunjukkan bahwa sedang mengakses alamat web www.globalsign.com

10.10.178.18.23 <-> 202.3.208.158

The screenshot shows the Wireshark Packet Decoder interface. The title bar reads "Packet Decoding - 10.178.18.23<->202.3.208.158 - Analysis Project 1". The interface includes navigation buttons (Previous, Next, Decoding View, Hex View, Layout1, Layout2) and a "Settings" button. The "Packet Info" pane shows the following details:

- Number: 55
- Packet Length: 459
- Capture Length: 459
- Timestamp: 2017/02/15 02:51:17.835097
- Ethernet Type II: [0/14]
- Destination Address: E4:8D:8C:21:90:18 (Routerboard.com) [0/6]
- Source Address: 50:B7:C3:D7:3E:B9 (Samsung Electronics CO., LTD) [6/6]

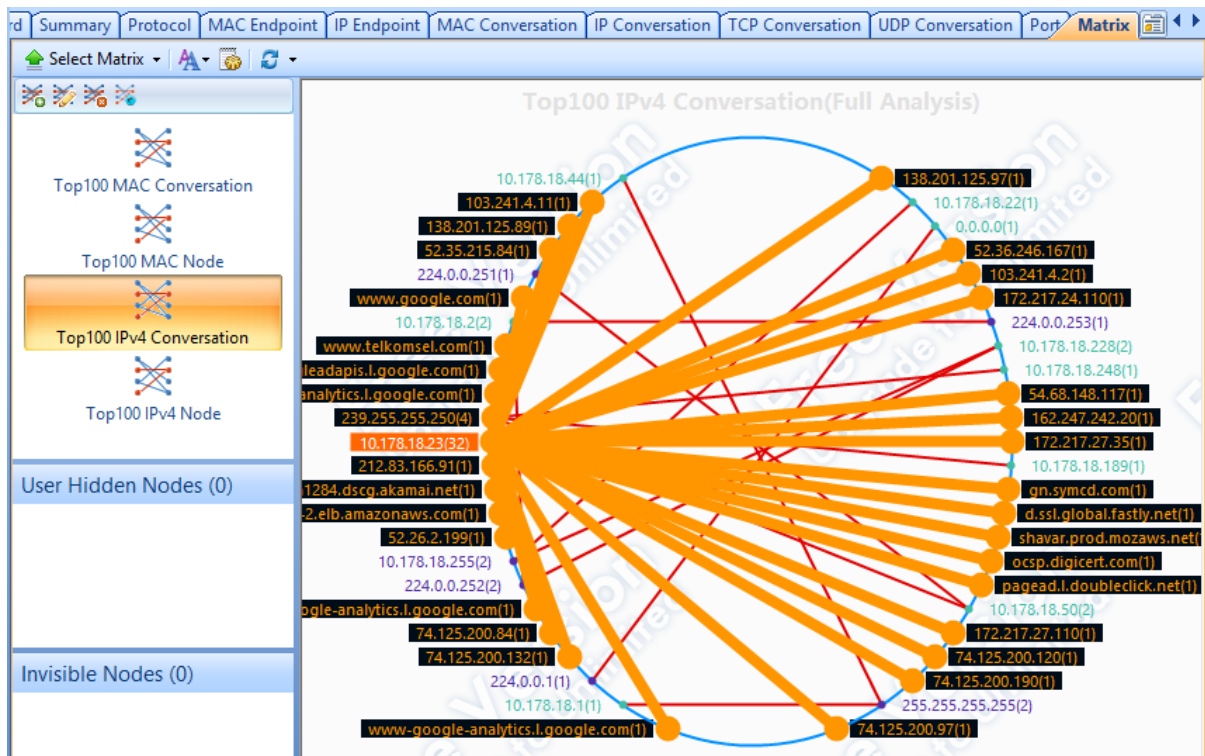
The packet bytes pane shows the raw data of the packet, which is an HTTP GET request. The first few bytes are: 00000000 E4 8D 8C 21 90 18 50 B7 C3 D7 3E B9 08 00 45 00 01 BD 50 1B 40 00 80 06 F1 B4 0A B2 12 17 CA. The corresponding ASCII text is: "...!..P...>...E...P.@.....". The rest of the packet contains the standard HTTP request headers and the request line: "GET / HTTP/1.1..Host: telkomsel.com..User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0..Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8..Accept-Language: en-US,en;q=0.5..Accept-Encoding: gzip, deflate..Cookie: _ga=GA1.2.1111667046.1487101564; _dc_gtm_UA-17788221-1=1; _gat_UA-17788221-1=1..Connection: keep-alive..Upgrade".

Hasil Analisis :

Berdasarkan tampilan diatas hasil komunikasi antara IP Address 10.178.18.23 dengan IP Address 202.3.208.158 menunjukkan bahwa sedang mengakses alamat web www.telkomsel.com

Matrix

Matrix menunjukkan representasi grafis dari semua percakapan yang ditangkap sepanjang sesi. Hal ini memungkinkan pemantauan percakapan endpoint dan secara otomatis akan menyelesaikan endpoint bila memungkinkan. Matrix terdiri dari panel kiri dan matriks yang elips merapat dengan node dan garis menghubungkan node, node adalah alamat MAC / IP dan garis mengindikasikan komunikasi antara alamat. Jumlah setelah node mewakili jumlah rekan host.



Hasil Analisis :

Berdasarkan tampilan diatas IP Address 10.178.18.23(23) menampilkan semua informasi yang relevan tentang komunikasi antara beberapa alamat/host. Diantaranya :

- 1. 10.178.18.23(23) <-> 74.125.200.100(1)**
mengakses alamat web www.google-analytics.com
- 2. 10.178.18.23(23) <-> 74.125.200.97(1)**
mengakses alamat web www.googletagmanager.com
- 3. 10.178.18.23(23) <-> 103.241.4.11(1)**
mengakses alamat web www.fonts.googleapis.com
- 4. 10.178.18.23(23) <-> 52.43.25.167(1)**
mengakses alamat web www.mozilla.org

5. **10.178.18.23(23) <-> 23.15.155.27(1)**
mengakses alamat web www.gn.symcd.com
6. **10.178.18.23(23) <-> 162.247.242.20(1)**
mengakses alamat web www.nr-data.net
7. **10.178.18.23(23) <-> 151.101.8.207(1)**
mengakses alamat web www.newrelic.com
8. **10.178.18.23(23) <-> 10.178.18.23(1)**
mengakses alamat web www.telkomsel.com