

KOMUNIKASI DATA DAN JARINGAN KOMPUTER

Analisis isi paket data dari 10 ip address



Disusun Oleh :

- Nama : Dodi Novembri
- NIM : 09031281520102
-

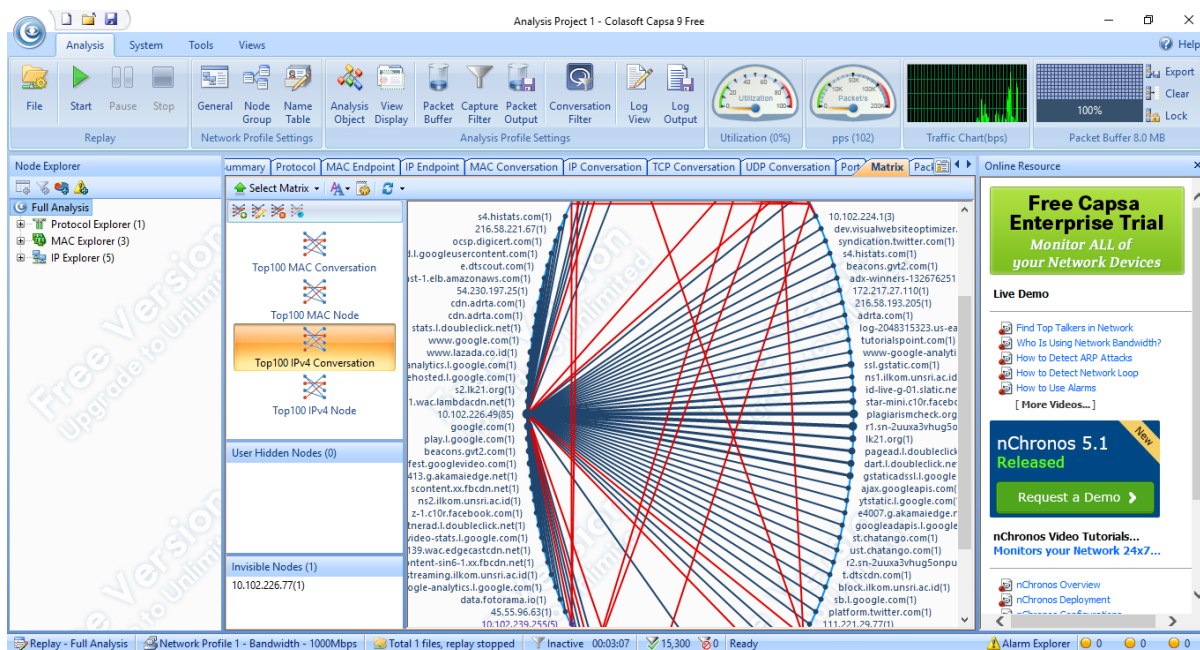
Dosen Pembimbing
Deris Stiawan, M. T., Ph.D

SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2017

Analisis isi paket data dari 10 ip address

Data didapatkan dari capture menggunakan wireshark yang kemudian dianalisis menggunakan colasoft capsap, ketika capture diaktifkan saya sedikit bermain pada beberapa website, isi data yang bisa di dapat yaitu sebagai berikut :



1. Isi paket dari IP Address source 10.102.226.49 ke destination 66.117.25.198 atau sebaliknya

Colasoft Capsa - TCP Flow Analysis - 10.102.226.49 - lazada.d3.sc.omtrdc.net - Analysis Project 1

```

...D.t(...4'..E..Rpu@...=^f.1Bu....P.6....
H"P...C...GET /b/ss/lazwebid/1/JS-1.4.1/s813
03608000066?AQB=1&ndh=1&pf=1&t=15%2F1%2F2017
%2015%3A22%3A26%203%20-420&mid=0450421171913
3951027790579983368663497&aamh=3&ce=UTF-8&n
s=lazada&fpCookieDomainPeriods=3&pageName=D%
3Dch%2B%22%3AIndexpage%22&g=http%3A%2F%2Fwww
.lazada.co.id%2F&r=https%3A%2F%2Fwww.google
.co.id%2F&cc=IDR&ch=index&server=www.lazada.c
o.id&aamb=hmk_Lq6TPIBMW925SPhw3Q&v1=Google&v
2=Search%20Engine%3A%20Organic&c5=D%3Dg&c7=D
%3Dv7&c8=D%3Dv8&v9=desktop&v10=ID&c11=D%3Dv2
8&c12=D%3Dv29&v12=0&c13=D%3Dv30&v13=new&c14=
detail%3Acasio-jam-tangan-ae-1000-w-lavdf-hi
tam-56368&v14=id&v15=0&v18=0&v20=Unknown&v24
=1&v25=First%20Visit&v28=4%3A00PM&v29=Wednes
day&v30=Weekday&v81=index&s=1366x768&c=24&j=
1.6&v=N&k=Y&bw=1366&bh=662&AQE=1 HTTP/1.1..H
ost: lazada.d3.sc.omtrdc.net..Connection: ke
ep-alive..User-Agent: Mozilla/5.0 (Windows N
T 10.0; Win64; x64) AppleWebKit/537.36 (KHTM
L, like Gecko) Chrome/56.0.2924.87 Safari/53
    
```

Dari gambar diatas dapat kita lihat kalau ip 10.102.226.49 mencoba untuk membuka www.lazada.co.id dari https google.co.id yang mana akses alamat tersebut terjadi pada hari rabu, kemudian membuka gambar jam tangan hitam yang berukuran 1366x768.

2. Isi paket dari IP Address source 10.102.226.49 ke destination 10.102.226.49 atau sebaliknya

Packet Decoding - 104.24.20.20<-> 10.102.226.49 - Analysis Project 1

```
(...4'...D.t..E..u..
@.4...h....f.1.P."I.
.AW.)P...;4..HTTP/1
.1 301 Moved Permanently..Date: Wed, 15 Feb 2017 08:46:44 GMT..Content-Type: text/html..Transfer-Encoding: chunked..Connection: keep-alive..Set-Cookie: __cfduid=db485fe2ebd0ad7a1f1573359e3cf05141487148404; expires=Thu, 15-Feb-18 08:46:44 GMT; path=/; domain=plagiarismcheck.org; HttpOnly..Location: https://plagiarismcheck.org/..Server: Cloudflare-nginx..CF-RAY: 33177db6a08431a4-SIN....b8...<html>..<head><title>301 Moved Permanently</title></head>..<body bgcolor="white">..<center><h1>301 Moved Permanently</h1></center>..<hr><center>nginx/1.9.4</center>..</body>..</html>....0.
...
```

Dari gambar dapat kita ketahui kalau tanggal diakses yaitu 15 februari 2017, alamat yang diakses yaitu plagiarismcheck.org serta menu yang dipilih yaitu moved permanently

3. Isi paket dari IP Address source 10.102.226.49 ke destination 66.117.25.198 atau sebaliknya

```
...D.t(...4'...E...p
.@...<V.f.1Bu....P
.....\P.....GET
/b/ss/lazwebid/1/J
S-1.4.1/s8613600796
3974?AQB=1&ndh=1&pf
=1&st=15%2F1%2F2017%
2015%3A46%3A13%203%
20-420&mid=04504211
7191339510277905799
83368663497&saamlh=3
&ce=UTF-8&ns=lazada
&fpCookieDomainPeri
ods=3&pageName=D%3D
ch%2B%22%3AAksesori
%20Komputer%22&g=h
ttp%3A%2F%2Fwww.laz
ada.co.id%2Fbeli-ak
sesori-komputer%2Ffa
cer%2F&r=http%3A%2F
%2Fwww.lazada.co.id
%2F&cc=IDR&pid=D%3D
ch%2B%22%3AIndexpag
e%22&pidt=1&oid=htt
p%3A%2F%2Fwww.lazad
a.co.id%2Fbeli-akse
sori-komputer%2FACE
r%2F&ot=A&ch=subcat
egory&server=www.la
zada.co.id&aamb=hmk
_Lq6TPIBMW925SPhw3Q
&l2=D%3Dc10&c5=D%3D
g&c7=D%3Dv7&c8=D%3D
```

Berdasarkan gambar diatas dapat diketahui bahwa ip address 10.102.226.49 mengakses situs lazada.co.id dan memilih pilihan aksesoris komputer

4. Isi paket dari IP Address source 10.102.226.49 ke destination 66.117.25.198 atau sebaliknya

```
...D.t(...4'..E....)
@.....f.lu.....P..
$Sa3i.P.....GET /
HTTP/1.1..Host: tuto
rialspoint.com..Conn
ection: keep-alive..
Upgrade-Insecure-Req
uests: 1..User-Agent
: Mozilla/5.0 (Windo
ws NT 10.0; Win64; x
64) AppleWebKit/537.
36 (KHTML, like Geck
o) Chrome/56.0.2924.
87 Safari/537.36..Ac
cept: text/html,appl
ication/xhtml+xml,ap
plication/xml;q=0.9,
image/webp,*/*;q=0.8
..Accept-Encoding: g
zip, deflate, sdch..
Accept-Language: en-
US,en;q=0.8....
```

Dari gambar diatas dapat dilihat kalau ip address 10.102.226.49 mengakses situs tutorialspoint.com

5. Isi paket dari IP Address source 10.102.226.49 ke destination 10.100.180.6 atau sebaliknya

```
/css/modern-respon
sive.css HTTP/1.1..
Host: streaming.il
kom.unsri.ac.id..Con
nection: keep-alive
..Cache-Control: ma
x-age=0..User-Agent
: Mozilla/5.0 (Wind
ows NT 10.0; Win64;
x64) AppleWebKit/5
37.36 (KHTML, like
Gecko) Chrome/56.0.
2924.87 Safari/537.
36..Accept: text/cs
s,*/*;q=0.1..Refer
er: http://block.il
kom.unsri.ac.id/..Ac
cept-Encoding: gzip
, deflate, sdch..Ac
cept-Language: en-U
S,en;q=0.8..Cookie:
sc_is_visitor_uniq
ue=rx10733571.14871
40743.EE6146F524534
F7CBC6ADBCC83902350
.1.1.1.1.1.1.1.1.1.1;
_ga=GA1.3.74470811
7.1486517444..If-No
ne-Match: "2160f90-
5538-5035147a84e40"
..If-Modified-Since
: Thu, 18 Sep 2014
```

Dari gambar dapat dilihat kalau ip address 10.102.226.49 mencoba mengakses streaming.ilkom.unsri.ac.id lalu berhasil ditandai dengan adanya keep-alive dan kemudian muncul link yang menampilkan block.ilkom.unsri.ac.id

6. Isi paket dari IP Address source 10.102.226.49 ke destination 93.184.215.177 atau sebaliknya

```
...D.t(...4'..E...[
.@...Q..f.1k..U...P
JJ:...{.QP...U...POS
T /impact/1/19870?r
nd=zqmfyasiwlllijwp
vdnsnyohnfdjtixb HT
TP/1.1..Host: rpt.c
edexis.com..Connect
ion: keep-alive..Co
ntent-Length: 176..
Origin: http://olx.
co.id..User-Agent:
Mozilla/5.0 (Window
s NT 10.0; Win64; x
64) AppleWebKit/537
.36 (KHTML, like Ge
cko) Chrome/56.0.29
24.87 Safari/537.36
..Content-Type: tex
t/plain;charset=UIF
-8..Accept: /*/*..Re
ferer: http://olx.c
o.id/properti/rumah
/dijual-rumah/..Acc
ept-Encoding: gzip,
deflate..Accept-La
nguage: en-US,en;q=
0.8....{"client":{"
type":"JS Impact Pl
ugin","version":"4.
0.0"},"dims":{"impa
ctSessionId":"37703
```

Dari gambar dapat diketahui kalau ip 10.102.226.49 mengakses rpt.cedexis.com lalu memilih content properti trus rumah

7. Isi paket dari IP Address source 10.102.226.49 ke destination 31.13.78.13 atau sebaliknya

```
...D.t(...4'..E...2DT
@...Z..f.1..N....Pn.
.(R.d7P....f..GET /h
ttp://jagatplay.com/
2017/02/news/tabata
ingin-rilis-final-fa
ntasy-xy-untuk-pc/ H
TTP/1.1..Host: graph
.facebook.com..Conne
ction: keep-alive..A
ccept: application/j
son, text/javascript
, /*/*; q=0.01..Origi
n: http://jagatplay.
com..User-Agent: Moz
illa/5.0 (Windows NT
10.0; Win64; x64) A
ppleWebKit/537.36 (K
HTML, like Gecko) Ch
rome/56.0.2924.87 Sa
fari/537.36..Referer
: http://jagatplay.c
om/2017/02/news/ta
bata-ingin-rilis-final
-fantasy-xy-untuk-pc
/..Accept-Encoding:
gzip, deflate, sdch.
.Accept-Language: en
-US,en;q=0.8....
```

Dari gambar dapat diketahui kalau ip 10.102.226.49 mengakses situs jagatplay.com lalu memilih content tabata ingin rilis final fantasy xy utuk pc dari ikon navbar news

8. Isi paket dari IP Address source 10.102.226.49 ke destination 103.20.94.1 atau sebaliknya

```
...D.t(...4'..E....
2@...1..f.lg.^....P
L;u9w..0P....y..GET
/countserv/count/s
hare?format=json&c
allback=jQuery11130
7023585015231297_14
87152987024&url=htt
p://jagatplay.com/2
017/02/news/miyamot
o-jelaskan-peran-me
ndiang-iwata-di-nis
tendo-switch/&_s=148
7152987025 HTTP/1.1
..Host: www.linkedi
n.com..Connection:
keep-alive..User-Ag
ent: Mozilla/5.0 (W
indows NT 10.0; Win
64; x64) AppleWebKit/537.36 (KHTML, li
ke Gecko) Chrome/56
.0.2924.87 Safari/5
37.36..Accept: */*.
.Referer: http://ja
gatplay.com/2017/02
/news/miyamoto-jela
skan-peran-mendiang
-iwata-di-nistendo-
switch/..Accept-Enc
```

Dari gambar dapat dilihat kalau ip 10.102.226.49 memilih content miyaoto jelaskan peran mendiangiwata di nistendo dari situs jagatplay.com

9. Isi paket dari IP Address source 10.102.226.49 ke destination 103.223.1.38 atau sebaliknya

```
(...4'...D.t..E...u-
@.4.z.g..&.f.l.P....
.&....P.....HTTP/1
.1 307 Temporary Red
irect..Server: nginx
..Date: Wed, 15 Feb
2017 05:04:49 GMT..C
ontent-Type: text/ht
ml..Content-Length:
180..Connection: kee
p-alive..Location: h
ttps://shopee.co.id/
....<html>..<head><t
itle>307 Temporary R
edirect</title></hea
d>..<body bgcolor="w
hite">..<center><h1>
307 Temporary Redire
ct</h1></center>..<h
r><center>nginx</cen
ter>..</body>..</htm
l>..
```

Dari gambar dapat dilihat kalau ip 10.102.226.49 mengakses shopee.co.id pada tanggal 15 februari 2016

10. Isi paket dari IP Address source 10.102.226.49 ke destination 103.223.1.38 atau sebaliknya

```
...D.t(...4'...E..yV-  
@.....f.1.:.....PF.  
..J.}.P.....GET /g  
tm.js?id=GTM-55FXG5  
HTTP/1.1. Host: www.  
googletagmanager.com  
..Connection: keep-a  
live..User-Agent: Mo  
zilla/5.0 (Windows N  
T 10.0; Win64; x64)  
AppleWebKit/537.36 (  
KHTML, like Gecko) C  
hrome/56.0.2924.87 S  
afari/537.36..Accept  
: /*..Referer: http  
://www.vans.com/..Ac  
cept-Encoding: gzip,  
deflate, sdch..Acce  
pt-Language: en-US,e  
n;q=0.8....
```

Dari gambar dapat dilihat kalau ip 10.102.226.49 mengakses www.googletagmanager.com dan juga mengakses www.vans.com pada tanggal 15 februari 2016