KEAMANAN JARINGAN KOMPUTER

“Cracking Password dan Try TOR BROWSER”

OLEH:

Doni Saputra (09011181520120)

Dosen Pengampuh : DERIS STIAWAN, M.T., PH.D.

Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

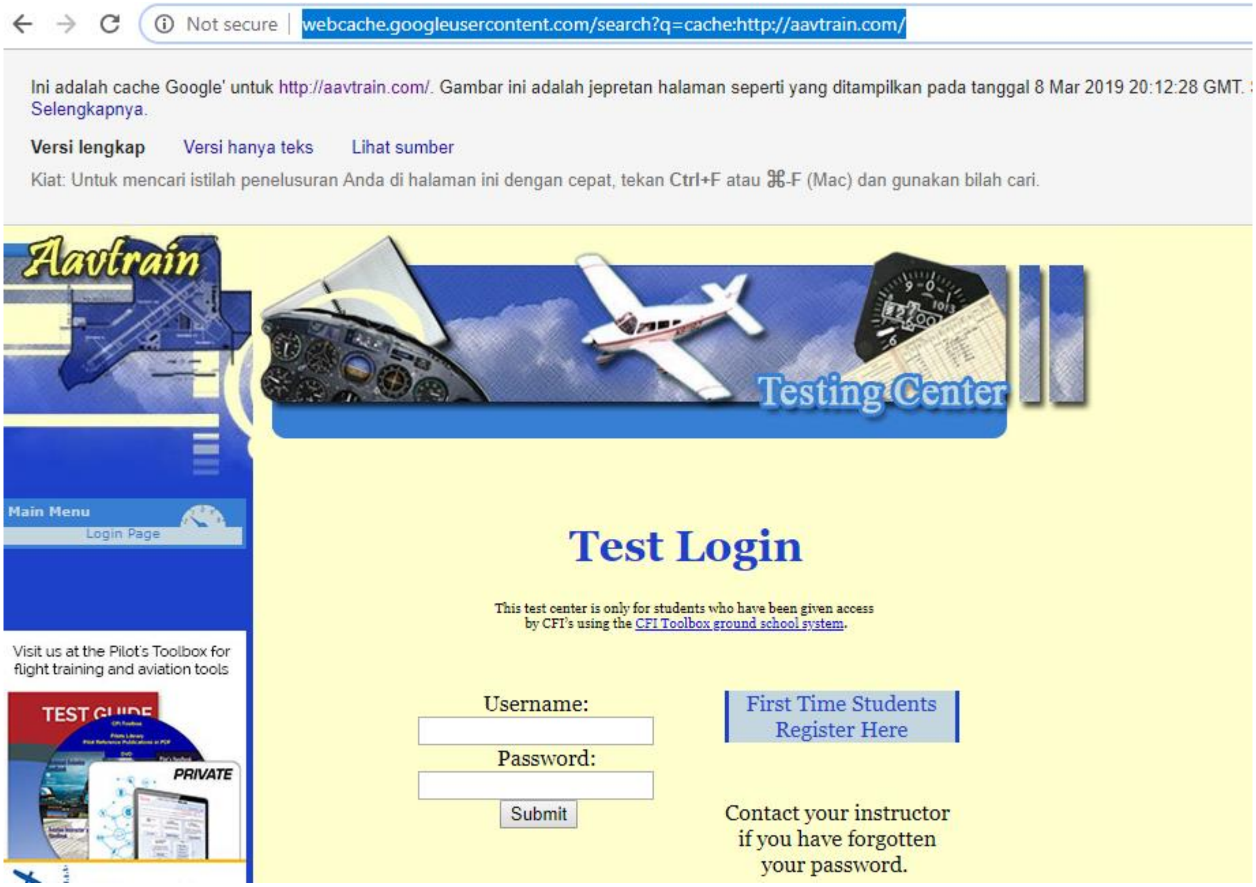
2019

1. CRACKING PASSWORD

Pada kasus ini menggunakan jaringan hotspot pribadi, 2 komputer sebagai attacker dan target. kemudian, **t**ools yang digunakan yaitu cain and abel dan wireshark. Pada kasus ini menggunakan 2 komputer dimana sebagai attacker dan target, tools cain and abel berfungsi untuk melakukan serangan pada komputer target yang mengakses http dan https. Kemudian dengan tools wireshark berfungsi untuk melihat aktivitas atau paket data yang ada pada komputer target.

a) HTTP

Website dengan protokol http yang diakses oleh target yaitu (http://webcache.googleusercontent.com/search?q=cache:http://aavtrain.com/).



Not secure
webcache.googleusercontent.com/search?q=cache:http://aavtrain.com/

Ini adalah cache Google' untuk http://aavtrain.com/. Gambar ini adalah jepretan halaman seperti yang ditampilkan pada tanggal 8 Mar 2019 20:12:28 GMT. Selengkapnya.

Kiat: Untuk mencari istilah penelusuran Anda di halaman ini dengan cepat, tekan Ctrl+F atau ⌘-F (Mac) dan gunakan bilah cari.

Test Login

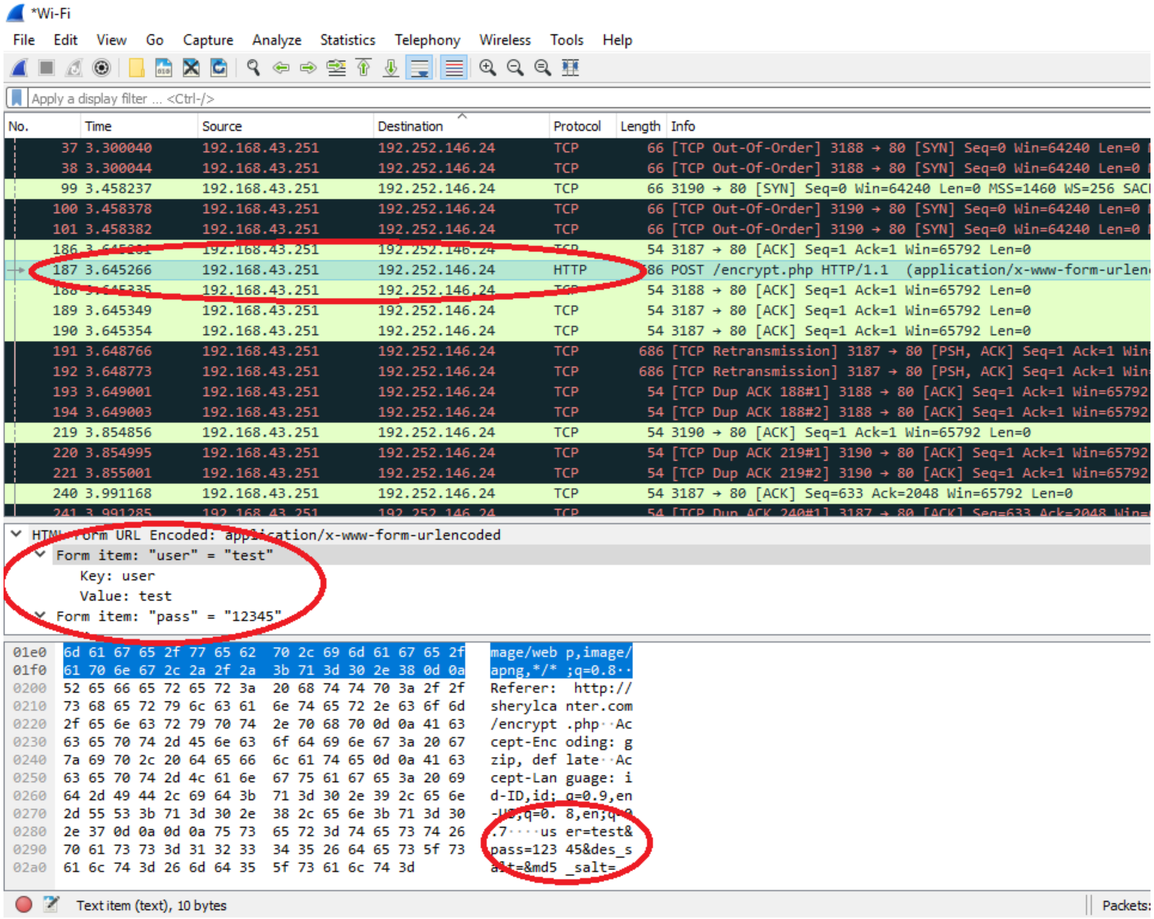
This test center is only for students who have been given access by CFI's using the CFI Toolbox ground school system.

Visit us at the Pilot's Toolbox for flight training and aviation tools

Contact your instructor if you have forgotten your password.

Gambar 1

Kemudian hasil yang didapat oleh attacker ketika target login pada website gambar 1 yaitu:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time       Source           Destination      Protocol  Length Info
     37 3.300040   192.168.43.251   192.252.146.24   TCP        66 [TCP Out-Of-Order] 3188 → 80 [SYN] Seq=0 Win=64240 Len=0
     38 3.300044   192.168.43.251   192.252.146.24   TCP        66 [TCP Out-Of-Order] 3188 → 80 [SYN] Seq=0 Win=64240 Len=0
     99 3.458237   192.168.43.251   192.252.146.24   TCP        66 3190 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
    100 3.458378   192.168.43.251   192.252.146.24   TCP        66 [TCP Out-Of-Order] 3190 → 80 [SYN] Seq=0 Win=64240 Len=0
    101 3.458382   192.168.43.251   192.252.146.24   TCP        66 [TCP Out-Of-Order] 3190 → 80 [SYN] Seq=0 Win=64240 Len=0
    186 3.645261   192.168.43.251   192.252.146.24   TCP        54 3187 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
    187 3.645266   192.168.43.251   192.252.146.24   HTTP      686 POST /encrypt.php HTTP/1.1  (application/x-www-form-urlen
    188 3.645335   192.168.43.251   192.252.146.24   TCP        54 3188 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
    189 3.645349   192.168.43.251   192.252.146.24   TCP        54 3187 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
    190 3.645354   192.168.43.251   192.252.146.24   TCP        54 3187 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
    191 3.648766   192.168.43.251   192.252.146.24   TCP       686 [TCP Retransmission] 3187 → 80 [PSH, ACK] Seq=1 Ack=1 Win
    192 3.648773   192.168.43.251   192.252.146.24   TCP       686 [TCP Retransmission] 3187 → 80 [PSH, ACK] Seq=1 Ack=1 Win
    193 3.649001   192.168.43.251   192.252.146.24   TCP        54 [TCP Dup ACK 188#1] 3188 → 80 [ACK] Seq=1 Ack=1 Win=65792
    194 3.649003   192.168.43.251   192.252.146.24   TCP        54 [TCP Dup ACK 188#2] 3188 → 80 [ACK] Seq=1 Ack=1 Win=65792
    219 3.854856   192.168.43.251   192.252.146.24   TCP        54 3190 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
    220 3.854995   192.168.43.251   192.252.146.24   TCP        54 [TCP Dup ACK 219#1] 3190 → 80 [ACK] Seq=1 Ack=1 Win=65792
    221 3.855001   192.168.43.251   192.252.146.24   TCP        54 [TCP Dup ACK 219#2] 3190 → 80 [ACK] Seq=1 Ack=1 Win=65792
    240 3.991168   192.168.43.251   192.252.146.24   TCP        54 3187 → 80 [ACK] Seq=633 Ack=2048 Win=65792 Len=0
    241 3.991285   192.168.43.251   192.252.146.24   TCP        54 [TCP Dup ACK 240#1] 3187 → 80 [ACK] Seq=633 Ack=2048 Win=
```

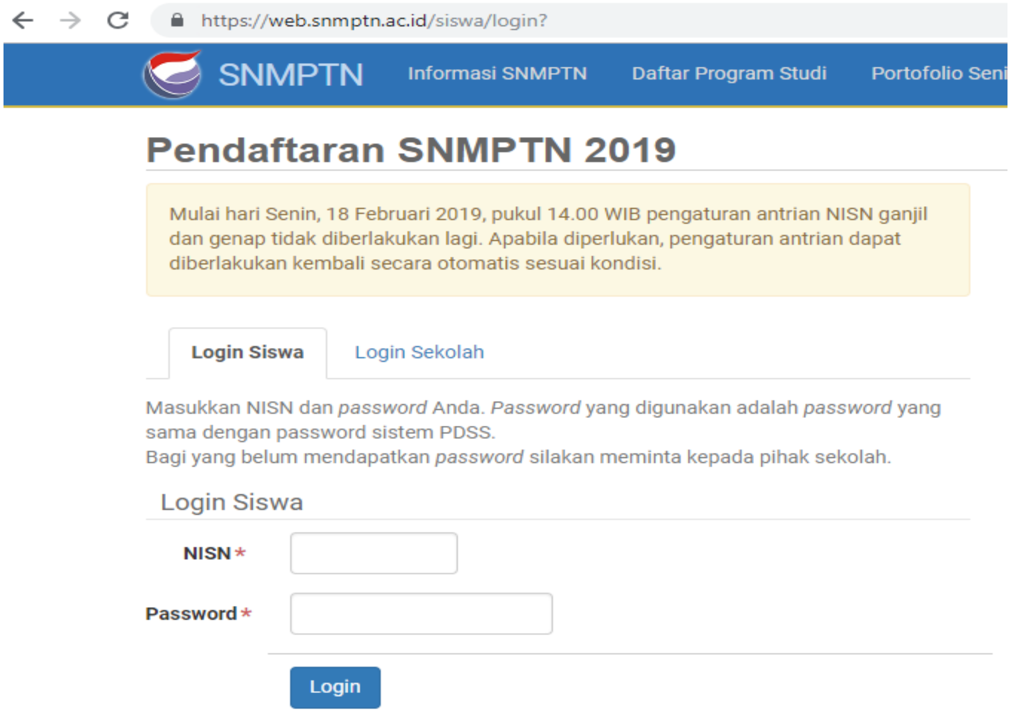
```
v HTML Form URL Encoded: application/x-www-form-urlencoded
  v Form item: "user" = "test"
      Key: user
      Value: test
  v Form item: "pass" = "12345"
```

```
01e0  6d 61 67 65 2f 77 65 62  70 2c 69 6d 61 67 65 2f   mage/web p,image/
01f0  61 70 6e 67 2c 2a 2f 2a  3b 71 3d 30 2e 38 0d 0a   apng,*/* ;q=0.8··
0200  52 65 66 65 72 65 72 3a  20 68 74 74 70 3a 2f 2f   Referer:  http://
0210  73 68 65 72 79 6c 63 61  6e 74 65 72 2e 63 6f 6d   sherylca nter.com
0220  2f 65 6e 63 72 79 70 74  2e 70 68 70 0d 0a 41 63   /encrypt .php··Ac
0230  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
0240  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 41 63   zip, def late··Ac
0250  63 65 70 74 2d 4c 61 6e  67 75 61 67 65 3a 20 69   cept-Lan guage: i
0260  64 2d 49 44 2c 69 64 3b  71 3d 30 2e 39 2c 65 6e   d-ID,id; q=0.9,en
0270  2d 55 53 3b 71 3d 30 2e  38 2c 65 6e 3b 71 3d 30   -US;q=0. 8,en;q=0
0280  2e 37 0d 0a 0d 0a 75 73  65 72 3d 74 65 73 74 26   .7····us er=test&
0290  70 61 73 73 3d 31 32 33  34 35 26 64 65 73 5f 73   pass=123 45&des_s
02a0  61 6c 74 3d 26 6d 64 35  5f 73 61 6c 74 3d         alt=&md5 _salt=
```

Gambar 2

IP 192.168.43.251 adalah target dan IP 192.252.146.24 adalah tujuan paket data dikirim. Pada saat target login website yang diakses maka akan ditangkap oleh tools cain and abel dan dengan tools wireshark didapatkan IP, tujuan, username dan password target. Dapat dilihat pada gambar 2.

b) HTTPS
Website dengan protokol https yang diakses oleh target yaitu (https://web.snmptn.ac.id/siswa/login?).



Pendaftaran SNMPTN 2019

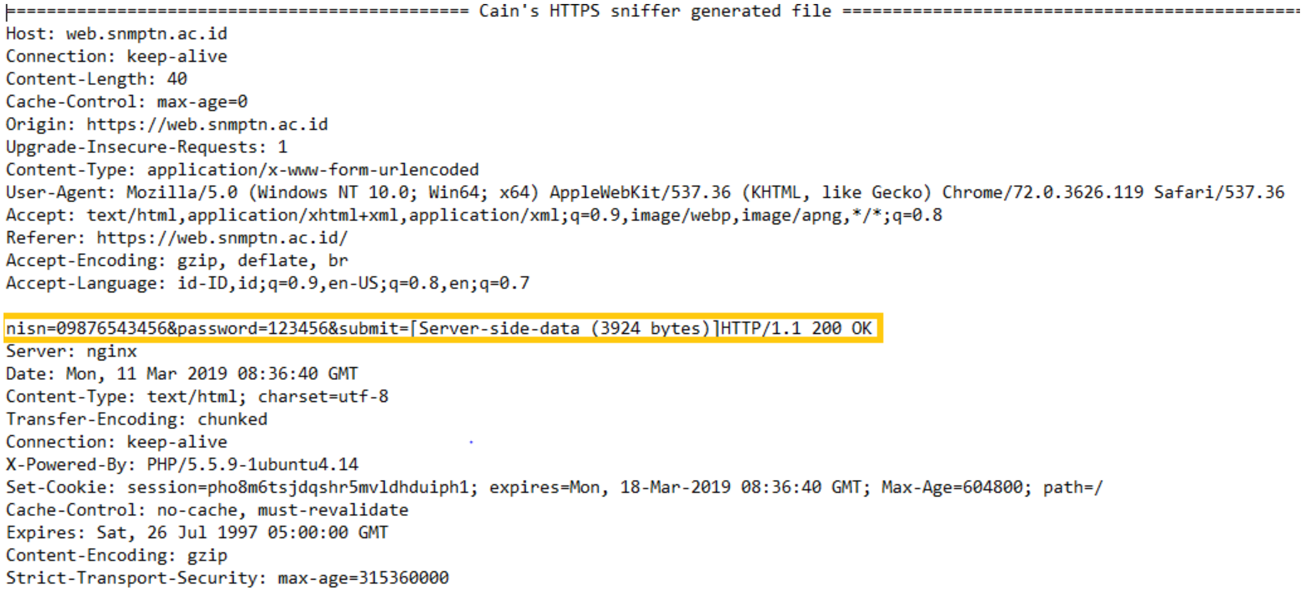
Mulai hari Senin, 18 Februari 2019, pukul 14.00 WIB pengaturan antrian NISN ganjil dan genap tidak diberlakukan lagi. Apabila diperlukan, pengaturan antrian dapat diberlakukan kembali secara otomatis sesuai kondisi.

Masukkan NISN dan *password* Anda. *Password* yang digunakan adalah *password* yang sama dengan password sistem PDSS.
Bagi yang belum mendapatkan *password* silakan meminta kepada pihak sekolah.

Login Siswa

Gambar 3

Kemudian hasil yang didapat oleh attacker ketika target login pada website gambar 3 yaitu:


```
============================================= Cain's HTTPS sniffer generated file =============================================
Host: web.snmptn.ac.id
Connection: keep-alive
Content-Length: 40
Cache-Control: max-age=0
Origin: https://web.snmptn.ac.id
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.119 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://web.snmptn.ac.id/
Accept-Encoding: gzip, deflate, br
Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7

nisn=09876543456&password=123456&submit=[Server-side-data (3924 bytes)]HTTP/1.1 200 OK
Server: nginx
Date: Mon, 11 Mar 2019 08:36:40 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Set-Cookie: session=pho8m6tsjdqshr5mvldhduiph1; expires=Mon, 18-Mar-2019 08:36:40 GMT; Max-Age=604800; path=/
Cache-Control: no-cache, must-revalidate
Expires: Sat, 26 Jul 1997 05:00:00 GMT
Content-Encoding: gzip
Strict-Transport-Security: max-age=315360000
```

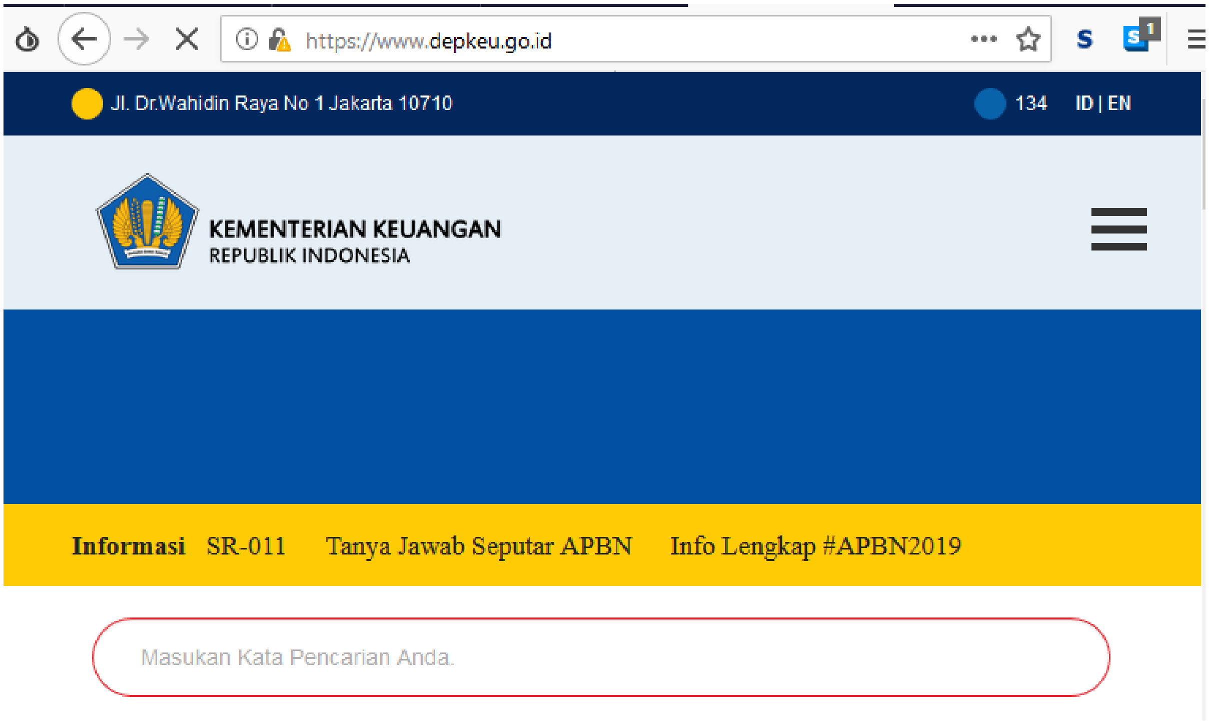
Gambar 4

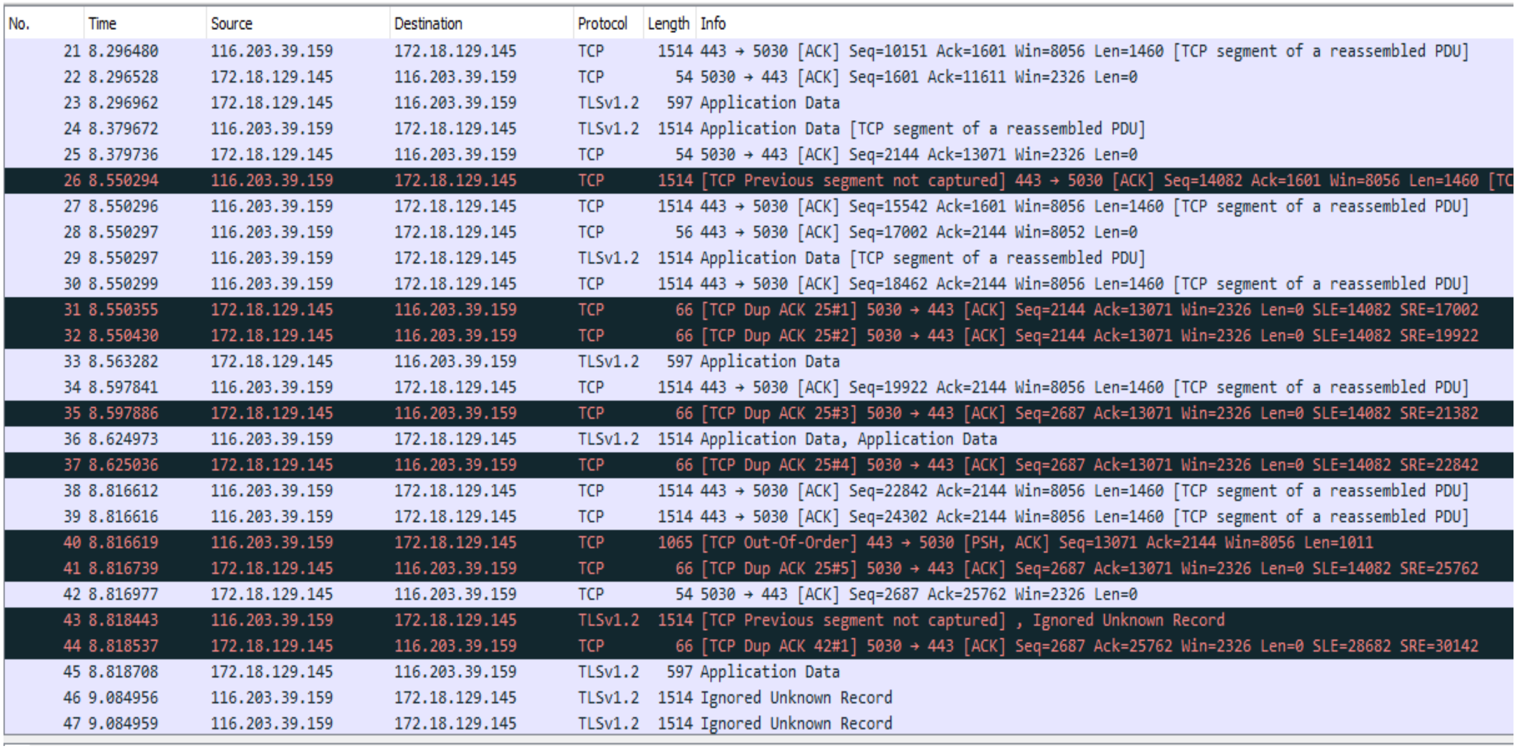
Pada protokol https karena sudah terenkripsi maka wireshark tidak menampilkan informasi yang dikirim dalam bentuk mentah, namun tools cain and abel dapat menampilkan informasi yang dikirim oleh target ke tujuan. Dapat dilihat pada gambar 4.

2. TRY TOR BROWSER

Jika dilihat melalui wireshark maka lalu lintas paket data sebagai berikut:

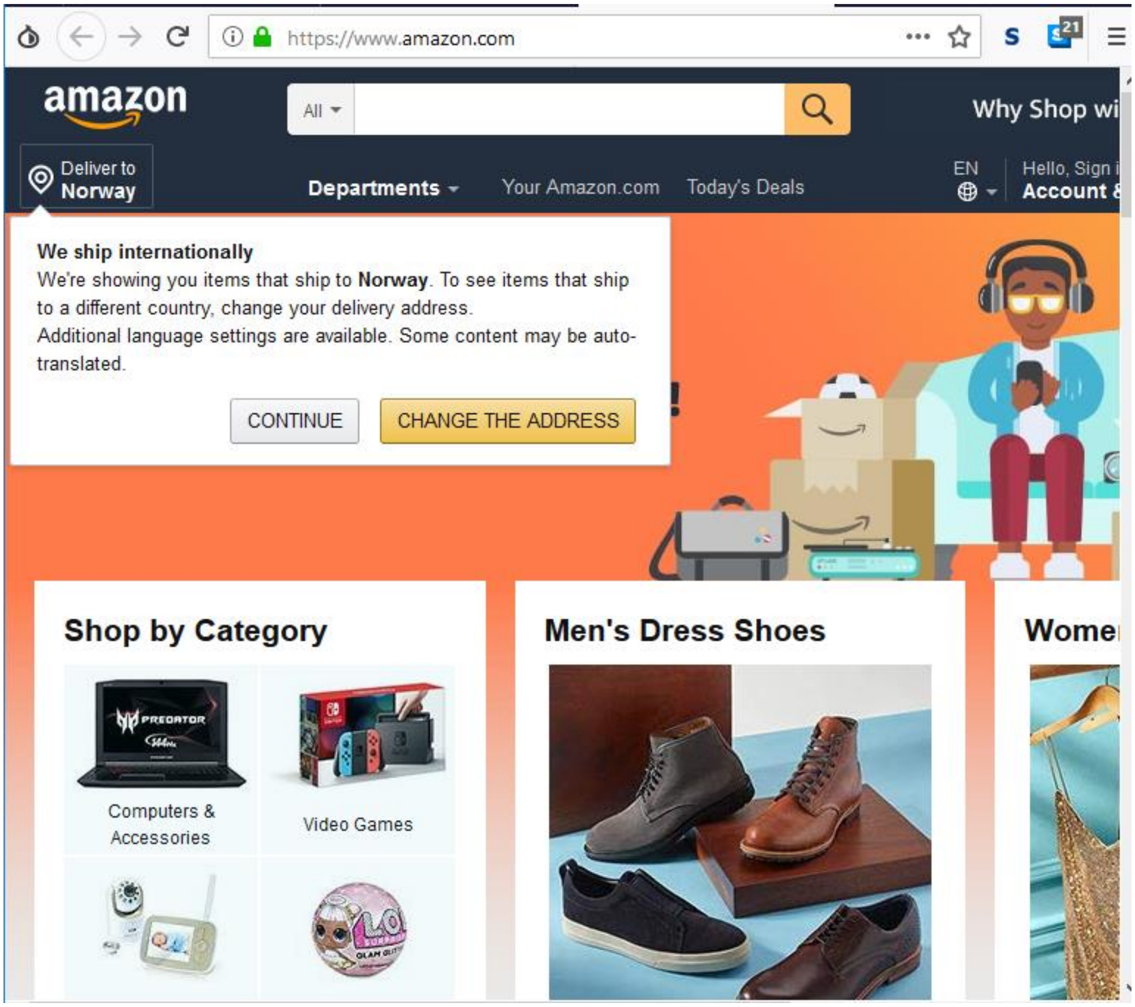
a) Website pemerintah (www.depkeu.go.id)





```
No.    Time        Source          Destination     Protocol Length Info
    21 8.296480    116.203.39.159  172.18.129.145  TCP      1514 443 → 5030 [ACK] Seq=10151 Ack=1601 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
    22 8.296528    172.18.129.145  116.203.39.159  TCP        54 5030 → 443 [ACK] Seq=1601 Ack=11611 Win=2326 Len=0
    23 8.296962    172.18.129.145  116.203.39.159  TLSv1.2   597 Application Data
    24 8.379672    116.203.39.159  172.18.129.145  TLSv1.2  1514 Application Data [TCP segment of a reassembled PDU]
    25 8.379736    172.18.129.145  116.203.39.159  TCP        54 5030 → 443 [ACK] Seq=2144 Ack=13071 Win=2326 Len=0
    26 8.550294    116.203.39.159  172.18.129.145  TCP      1514 [TCP Previous segment not captured] 443 → 5030 [ACK] Seq=14082 Ack=1601 Win=8056 Len=1460 [TC
    27 8.550296    116.203.39.159  172.18.129.145  TCP      1514 443 → 5030 [ACK] Seq=15542 Ack=1601 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
    28 8.550297    116.203.39.159  172.18.129.145  TCP        56 443 → 5030 [ACK] Seq=17002 Ack=2144 Win=8052 Len=0
    29 8.550297    116.203.39.159  172.18.129.145  TLSv1.2  1514 Application Data [TCP segment of a reassembled PDU]
    30 8.550299    116.203.39.159  172.18.129.145  TCP      1514 443 → 5030 [ACK] Seq=18462 Ack=2144 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
    31 8.550355    172.18.129.145  116.203.39.159  TCP        66 [TCP Dup ACK 25#1] 5030 → 443 [ACK] Seq=2144 Ack=13071 Win=2326 Len=0 SLE=14082 SRE=17002
    32 8.550430    172.18.129.145  116.203.39.159  TCP        66 [TCP Dup ACK 25#2] 5030 → 443 [ACK] Seq=2144 Ack=13071 Win=2326 Len=0 SLE=14082 SRE=19922
    33 8.563282    172.18.129.145  116.203.39.159  TLSv1.2   597 Application Data
    34 8.597841    116.203.39.159  172.18.129.145  TCP      1514 443 → 5030 [ACK] Seq=19922 Ack=2144 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
    35 8.597886    172.18.129.145  116.203.39.159  TCP        66 [TCP Dup ACK 25#3] 5030 → 443 [ACK] Seq=2687 Ack=13071 Win=2326 Len=0 SLE=14082 SRE=21382
    36 8.624973    116.203.39.159  172.18.129.145  TLSv1.2  1514 Application Data, Application Data
    37 8.625036    172.18.129.145  116.203.39.159  TCP        66 [TCP Dup ACK 25#4] 5030 → 443 [ACK] Seq=2687 Ack=13071 Win=2326 Len=0 SLE=14082 SRE=22842
    38 8.816612    116.203.39.159  172.18.129.145  TCP      1514 443 → 5030 [ACK] Seq=22842 Ack=2144 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
    39 8.816616    116.203.39.159  172.18.129.145  TCP      1514 443 → 5030 [ACK] Seq=24302 Ack=2144 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
    40 8.816619    116.203.39.159  172.18.129.145  TCP      1065 [TCP Out-Of-Order] 443 → 5030 [PSH, ACK] Seq=13071 Ack=2144 Win=8056 Len=1011
    41 8.816739    172.18.129.145  116.203.39.159  TCP        66 [TCP Dup ACK 25#5] 5030 → 443 [ACK] Seq=2687 Ack=13071 Win=2326 Len=0 SLE=14082 SRE=25762
    42 8.816977    172.18.129.145  116.203.39.159  TCP        54 5030 → 443 [ACK] Seq=2687 Ack=25762 Win=2326 Len=0
    43 8.818443    116.203.39.159  172.18.129.145  TLSv1.2  1514 [TCP Previous segment not captured] , Ignored Unknown Record
    44 8.818537    172.18.129.145  116.203.39.159  TCP        66 [TCP Dup ACK 42#1] 5030 → 443 [ACK] Seq=2687 Ack=25762 Win=2326 Len=0 SLE=28682 SRE=30142
    45 8.818708    172.18.129.145  116.203.39.159  TLSv1.2   597 Application Data
    46 9.084956    116.203.39.159  172.18.129.145  TLSv1.2  1514 Ignored Unknown Record
    47 9.084959    116.203.39.159  172.18.129.145  TLSv1.2  1514 Ignored Unknown Record
```

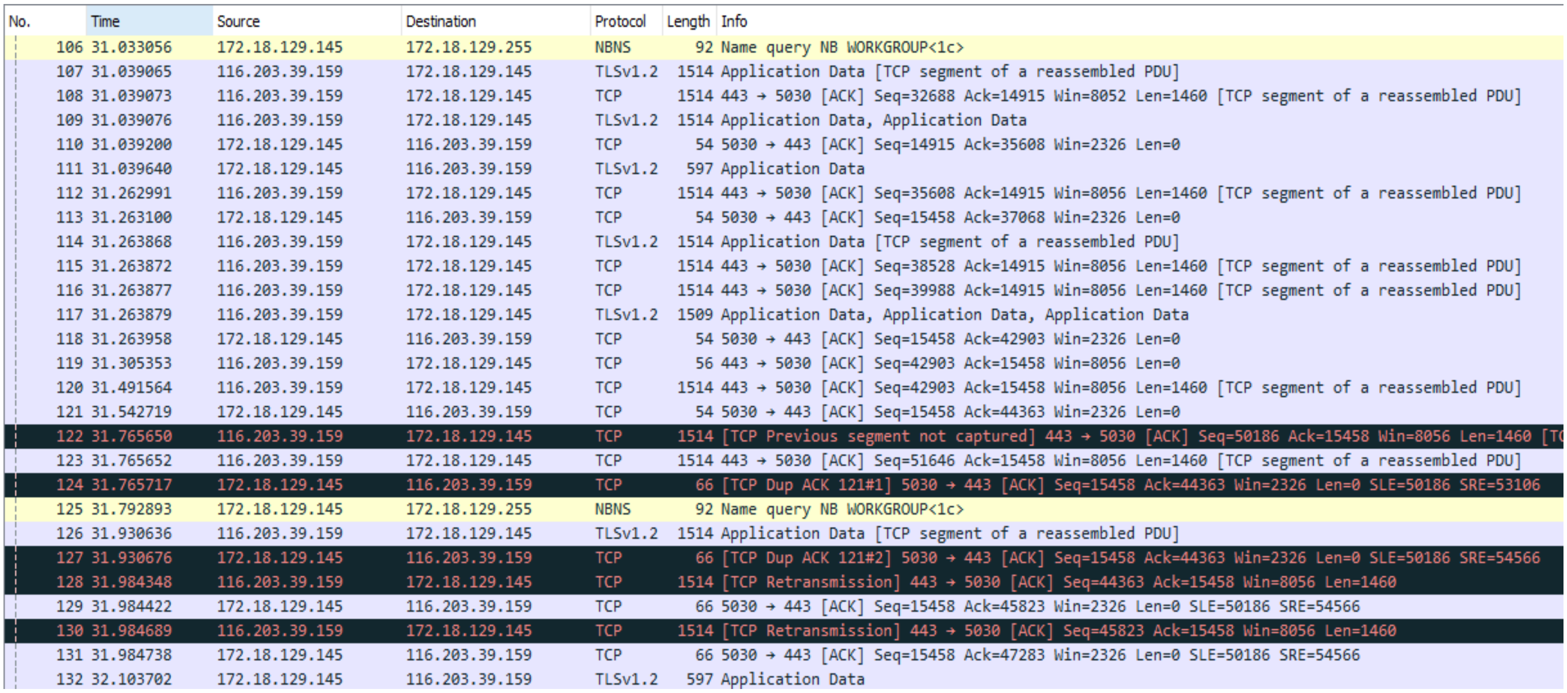
b) Website luar negeri (www.amazon.com)



We ship internationally

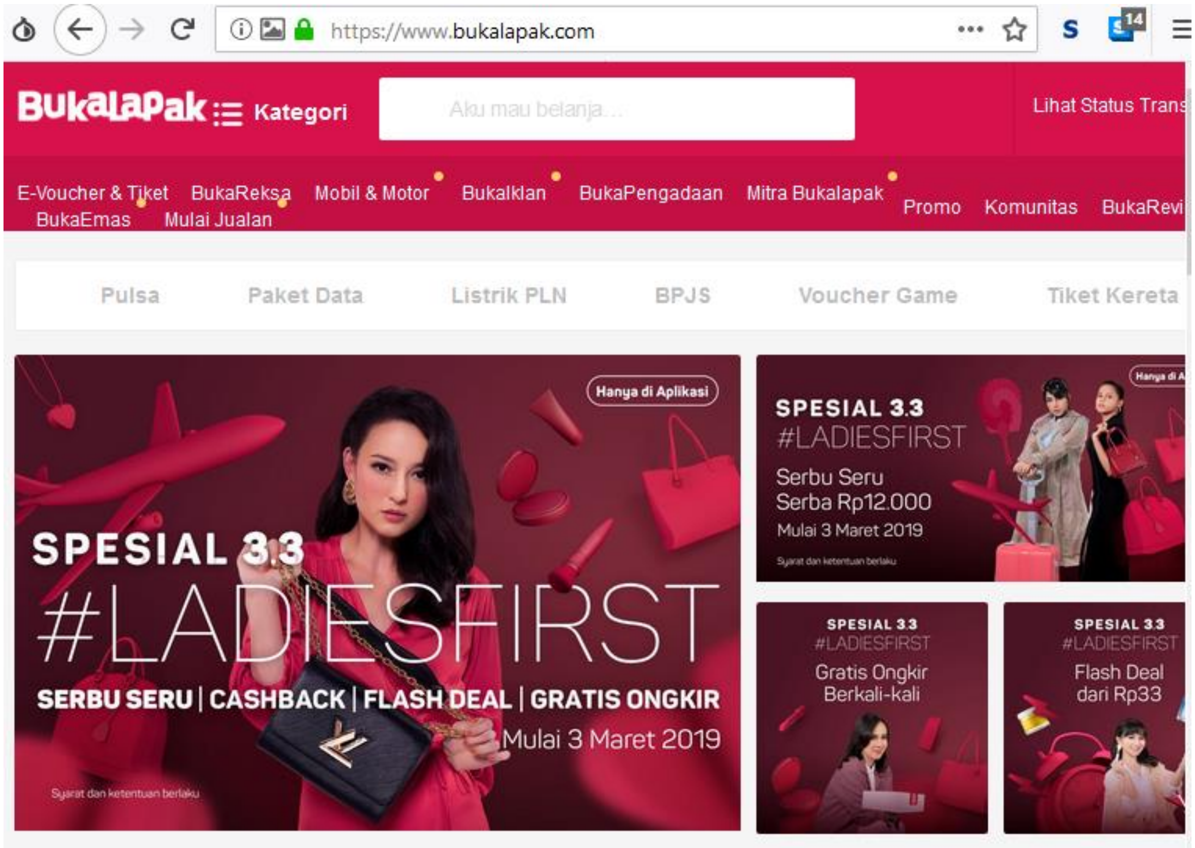
We're showing you items that ship to **Norway**. To see items that ship to a different country, change your delivery address.

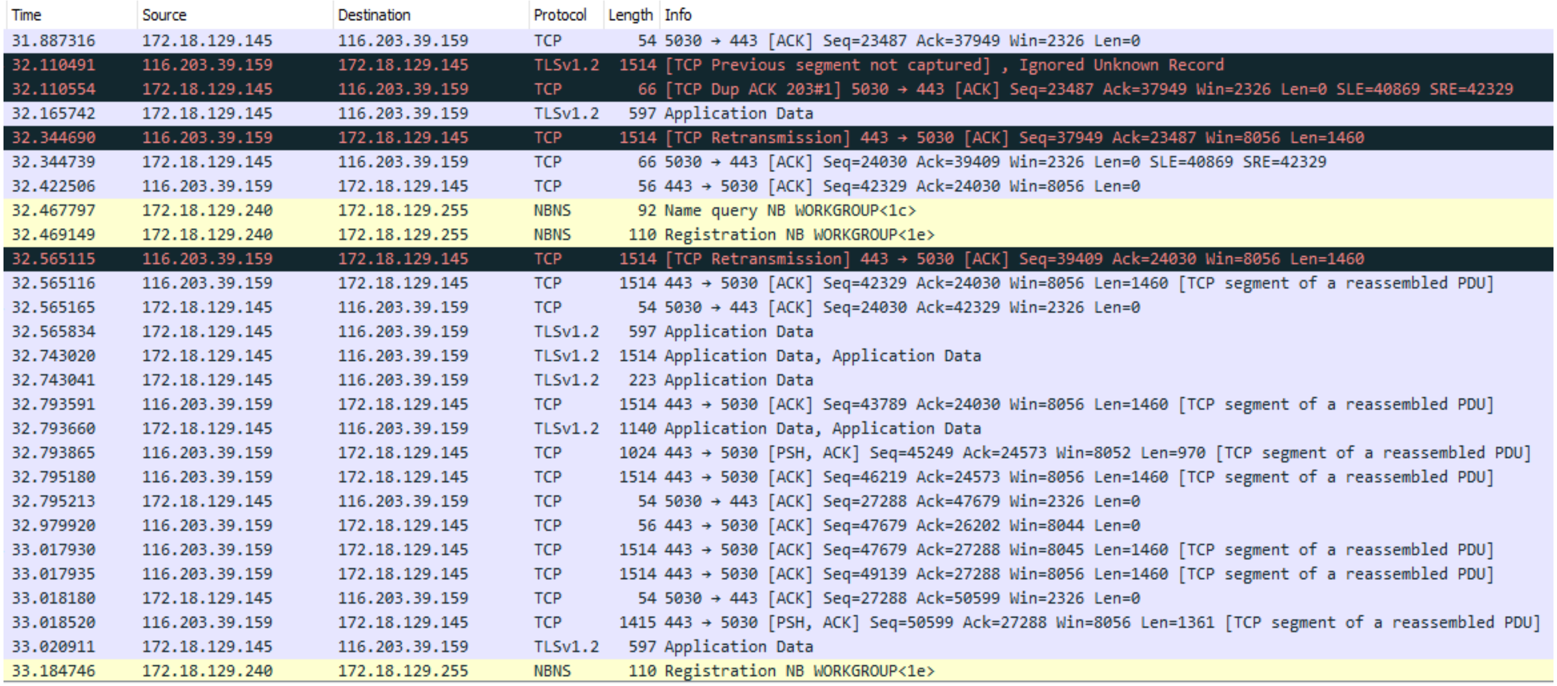
Additional language settings are available. Some content may be auto-translated.



```
No.     Time        Source           Destination      Protocol  Length Info
    106 31.033056   172.18.129.145   172.18.129.255   NBNS        92 Name query NB WORKGROUP<1c>
    107 31.039065   116.203.39.159   172.18.129.145   TLSv1.2   1514 Application Data [TCP segment of a reassembled PDU]
    108 31.039073   116.203.39.159   172.18.129.145   TCP       1514 443 → 5030 [ACK] Seq=32688 Ack=14915 Win=8052 Len=1460 [TCP segment of a reassembled PDU]
    109 31.039076   116.203.39.159   172.18.129.145   TLSv1.2   1514 Application Data, Application Data
    110 31.039200   172.18.129.145   116.203.39.159   TCP         54 5030 → 443 [ACK] Seq=14915 Ack=35608 Win=2326 Len=0
    111 31.039640   172.18.129.145   116.203.39.159   TLSv1.2    597 Application Data
    112 31.262991   116.203.39.159   172.18.129.145   TCP       1514 443 → 5030 [ACK] Seq=35608 Ack=14915 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
    113 31.263100   172.18.129.145   116.203.39.159   TCP         54 5030 → 443 [ACK] Seq=15458 Ack=37068 Win=2326 Len=0
    114 31.263868   116.203.39.159   172.18.129.145   TLSv1.2   1514 Application Data [TCP segment of a reassembled PDU]
    115 31.263872   116.203.39.159   172.18.129.145   TCP       1514 443 → 5030 [ACK] Seq=38528 Ack=14915 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
    116 31.263877   116.203.39.159   172.18.129.145   TCP       1514 443 → 5030 [ACK] Seq=39988 Ack=14915 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
    117 31.263879   116.203.39.159   172.18.129.145   TLSv1.2   1509 Application Data, Application Data, Application Data
    118 31.263958   172.18.129.145   116.203.39.159   TCP         54 5030 → 443 [ACK] Seq=15458 Ack=42903 Win=2326 Len=0
    119 31.305353   116.203.39.159   172.18.129.145   TCP         56 443 → 5030 [ACK] Seq=42903 Ack=15458 Win=8056 Len=0
    120 31.491564   116.203.39.159   172.18.129.145   TCP       1514 443 → 5030 [ACK] Seq=42903 Ack=15458 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
    121 31.542719   172.18.129.145   116.203.39.159   TCP         54 5030 → 443 [ACK] Seq=15458 Ack=44363 Win=2326 Len=0
    122 31.765650   116.203.39.159   172.18.129.145   TCP       1514 [TCP Previous segment not captured] 443 → 5030 [ACK] Seq=50186 Ack=15458 Win=8056 Len=1460 [TC
    123 31.765652   116.203.39.159   172.18.129.145   TCP       1514 443 → 5030 [ACK] Seq=51646 Ack=15458 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
    124 31.765717   172.18.129.145   116.203.39.159   TCP         66 [TCP Dup ACK 121#1] 5030 → 443 [ACK] Seq=15458 Ack=44363 Win=2326 Len=0 SLE=50186 SRE=53106
    125 31.792893   172.18.129.145   172.18.129.255   NBNS        92 Name query NB WORKGROUP<1c>
    126 31.930636   116.203.39.159   172.18.129.145   TLSv1.2   1514 Application Data [TCP segment of a reassembled PDU]
    127 31.930676   172.18.129.145   116.203.39.159   TCP         66 [TCP Dup ACK 121#2] 5030 → 443 [ACK] Seq=15458 Ack=44363 Win=2326 Len=0 SLE=50186 SRE=54566
    128 31.984348   116.203.39.159   172.18.129.145   TCP       1514 [TCP Retransmission] 443 → 5030 [ACK] Seq=44363 Ack=15458 Win=8056 Len=1460
    129 31.984422   172.18.129.145   116.203.39.159   TCP         66 5030 → 443 [ACK] Seq=15458 Ack=45823 Win=2326 Len=0 SLE=50186 SRE=54566
    130 31.984689   116.203.39.159   172.18.129.145   TCP       1514 [TCP Retransmission] 443 → 5030 [ACK] Seq=45823 Ack=15458 Win=8056 Len=1460
    131 31.984738   172.18.129.145   116.203.39.159   TCP         66 5030 → 443 [ACK] Seq=15458 Ack=47283 Win=2326 Len=0 SLE=50186 SRE=54566
    132 32.103702   172.18.129.145   116.203.39.159   TLSv1.2    597 Application Data
```

c) Website dalam negeri (bukalapak.com)





```
Time        Source          Destination     Protocol Length Info
31.887316   172.18.129.145  116.203.39.159  TCP        54 5030 → 443 [ACK] Seq=23487 Ack=37949 Win=2326 Len=0
32.110491   116.203.39.159  172.18.129.145  TLSv1.2  1514 [TCP Previous segment not captured] , Ignored Unknown Record
32.110554   172.18.129.145  116.203.39.159  TCP        66 [TCP Dup ACK 203#1] 5030 → 443 [ACK] Seq=23487 Ack=37949 Win=2326 Len=0 SLE=40869 SRE=42329
32.165742   172.18.129.145  116.203.39.159  TLSv1.2   597 Application Data
32.344690   116.203.39.159  172.18.129.145  TCP      1514 [TCP Retransmission] 443 → 5030 [ACK] Seq=37949 Ack=23487 Win=8056 Len=1460
32.344739   172.18.129.145  116.203.39.159  TCP        66 5030 → 443 [ACK] Seq=24030 Ack=39409 Win=2326 Len=0 SLE=40869 SRE=42329
32.422506   116.203.39.159  172.18.129.145  TCP        56 443 → 5030 [ACK] Seq=42329 Ack=24030 Win=8056 Len=0
32.467797   172.18.129.240  172.18.129.255  NBNS       92 Name query NB WORKGROUP<1c>
32.469149   172.18.129.240  172.18.129.255  NBNS      110 Registration NB WORKGROUP<1e>
32.565115   116.203.39.159  172.18.129.145  TCP      1514 [TCP Retransmission] 443 → 5030 [ACK] Seq=39409 Ack=24030 Win=8056 Len=1460
32.565116   116.203.39.159  172.18.129.145  TCP      1514 443 → 5030 [ACK] Seq=42329 Ack=24030 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
32.565165   172.18.129.145  116.203.39.159  TCP        54 5030 → 443 [ACK] Seq=24030 Ack=42329 Win=2326 Len=0
32.565834   172.18.129.145  116.203.39.159  TLSv1.2   597 Application Data
32.743020   172.18.129.145  116.203.39.159  TLSv1.2  1514 Application Data, Application Data
32.743041   172.18.129.145  116.203.39.159  TLSv1.2   223 Application Data
32.793591   116.203.39.159  172.18.129.145  TCP      1514 443 → 5030 [ACK] Seq=43789 Ack=24030 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
32.793660   172.18.129.145  116.203.39.159  TLSv1.2  1140 Application Data, Application Data
32.793865   116.203.39.159  172.18.129.145  TCP      1024 443 → 5030 [PSH, ACK] Seq=45249 Ack=24573 Win=8052 Len=970 [TCP segment of a reassembled PDU]
32.795180   116.203.39.159  172.18.129.145  TCP      1514 443 → 5030 [ACK] Seq=46219 Ack=24573 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
32.795213   172.18.129.145  116.203.39.159  TCP        54 5030 → 443 [ACK] Seq=27288 Ack=47679 Win=2326 Len=0
32.979920   116.203.39.159  172.18.129.145  TCP        56 443 → 5030 [ACK] Seq=47679 Ack=26202 Win=8044 Len=0
33.017930   116.203.39.159  172.18.129.145  TCP      1514 443 → 5030 [ACK] Seq=47679 Ack=27288 Win=8045 Len=1460 [TCP segment of a reassembled PDU]
33.017935   116.203.39.159  172.18.129.145  TCP      1514 443 → 5030 [ACK] Seq=49139 Ack=27288 Win=8056 Len=1460 [TCP segment of a reassembled PDU]
33.018180   172.18.129.145  116.203.39.159  TCP        54 5030 → 443 [ACK] Seq=27288 Ack=50599 Win=2326 Len=0
33.018520   116.203.39.159  172.18.129.145  TCP      1415 443 → 5030 [PSH, ACK] Seq=50599 Ack=27288 Win=8056 Len=1361 [TCP segment of a reassembled PDU]
33.020911   172.18.129.145  116.203.39.159  TLSv1.2   597 Application Data
33.184746   172.18.129.240  172.18.129.255  NBNS      110 Registration NB WORKGROUP<1e>
```