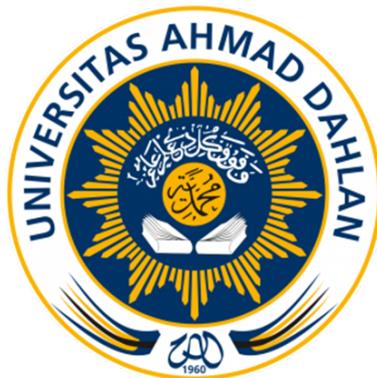


LAPORAN PRAKTIKUM

“Pertemuan ke-13: Keamanan Jaringan”

Diajukan untuk memenuhi salah satu praktikum Mata kuliah Praktikum Komunikasi Data dan Jaringan Komputer yang di ampu oleh:

Taufiq Ismail, S.T., M.Cs.



Disusun Oleh:

Mohammad Farid Hendianto 2200018401

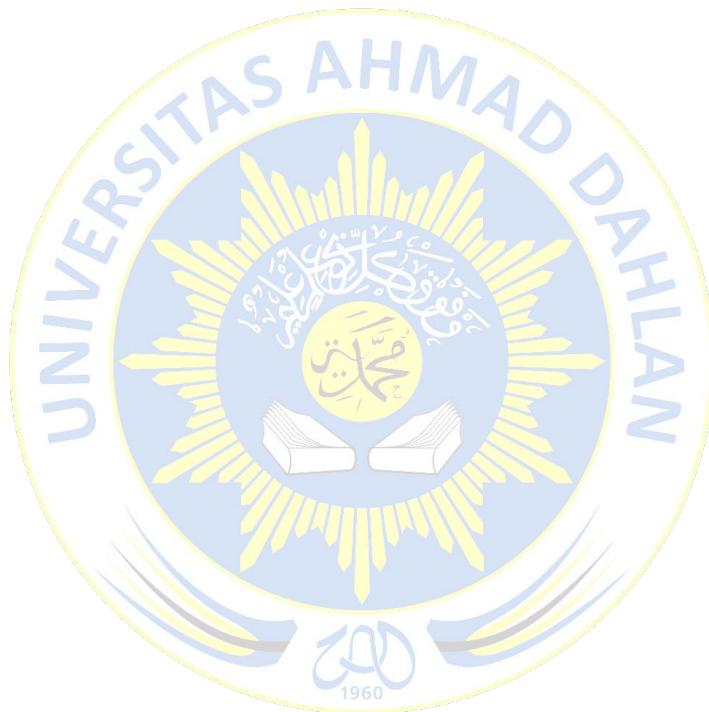
A / Senin 07.00 – 10.00 Lab. Multimedia

PJ: Reza

**PROGRAM STUDI INFORMATIKA
UNIVERSITAS AHMAD DAHLAN
FAKULTAS TEKNOLOGI INDUSTRI
TAHUN 2024**

DAFTAR ISI

PRETEST	3
LANGKAH PRAKTIKUM.....	4
POST TEST	8



PRETEST

1. Jelaskan kegunaan Wireshark (Minimal 2)!
2. Jelaskan perbedaan HTTP dan HTTPS!
3. Jelaskan yang dimaksud dengan TCP!

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama: Mohammad Farid H. NIM: 2200018401	Asisten: Paraf Asisten:	Tanggal: 04 Juli 2024 Nilai:
--	----------------------------	---------------------------------

1. Kegunaan wireshark antara lain:

- Wireshark merupakan alat administrator jaringan untuk memantau lalu lintas jaringan dan mendekomponsi masalah seperti keterlambatan jaringan, kehilangan paket atau kesalahan konfigurasi.
- Alat ini membantu dalam mendiagnosis dan menyelesaikan masalah jaringan dengan memungkinkan analisis tindak tentang berbagai data bersifat seluler di jaringan.
- Wireshark dapat digunakan untuk mendekomposisi serangan jaringan atau aktivitas melukiharmoni dengan menggunakan bila lalu lintas jaringan.
- Wireshark adalah alat yang berguna untuk mempelajari tentang protokol jaringan dan cara kerja jaringan. Banyak kursus jaringan dan komputer komputer.
- Pengembangan perangkat lunak dapat menggunakan wireshark untuk memudahkan bahasa aplikasi mereka berkomunikasi dengan teknologi sinyal.

2. Berikut adalah perbedaan antara HTTP dan HTTPS

HTTP (Hypertext Transfer Protocol) HTTPS (Hypertext Transfer Protocol Secure)

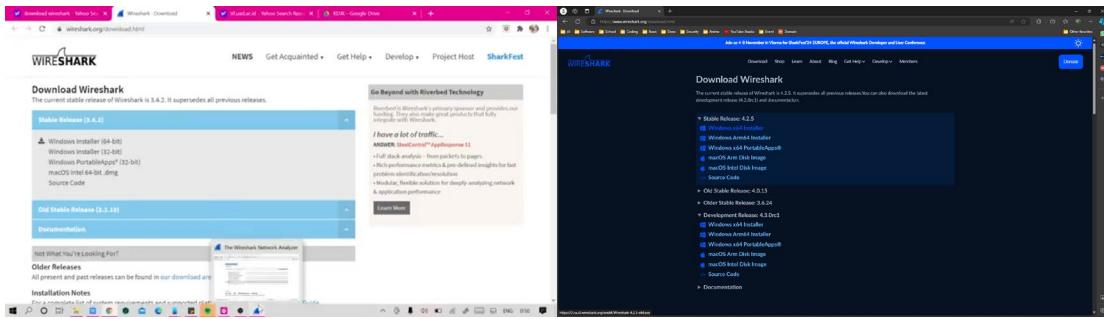
Keamanan	<ul style="list-style-type: none"> • Data dikirim dalam teks biasa • Data dilengkapi menggunakan SSL/TLS
Port yang digunakan	<ul style="list-style-type: none"> • Port 80 • Port 443
Sertifikat	<ul style="list-style-type: none"> • Tidak memerlukan sertifikat digital • Memerlukan sertifikat digital oleh operator sertifikat (CA)
Indikator di browser	<ul style="list-style-type: none"> • Tidak memfilter ikon • Memfilter ikon menjadi dibilah alamat
Penggunaan	<ul style="list-style-type: none"> • Lebih umum digunakan untuk tampilan yang tidak memerlukan keamanan tinggi. • Dianjurkan pada situs yang membutuhkan keamanan tinggi seperti bank atau login pengguna.

3. TCP (Transmission Control Protocol) adalah salah satu protokol utama dalam suite protokol internet (IP) yang digunakan untuk mengirimkan data angka ke komputer dalam jaringan. TCP berbentuk protokol yang berorientasi pada konversi, yang berarti setelah data dikirim, harus ada balasan (acknowledgement) yang dikirimkan dari titik akhir (meskipun antara titik dan sebaliknya).

Dan yang dimaksud dengan TCP atau sempai perempuan dalam artian yang belum menerima pasti mungkin tidak diizinkan yang berbeda,

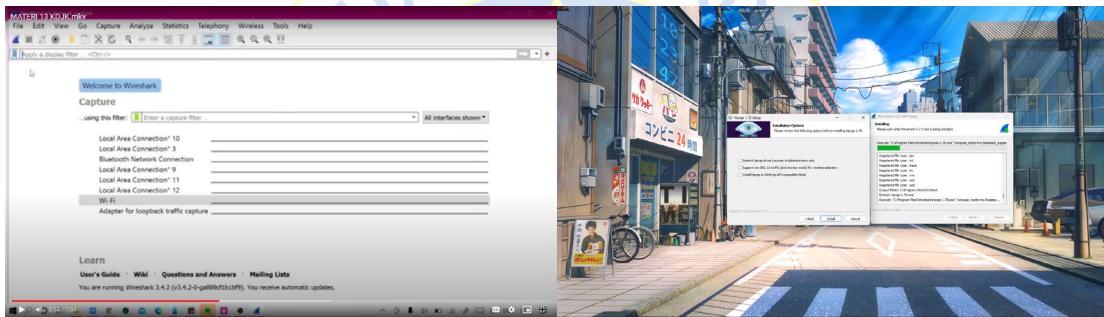
LANGKAH PRAKTIKUM

Download wireshark



Gambar 1 download Wireshark di <https://www.wireshark.org/download.html>

Mengunduh installer di website resmi Wireshark



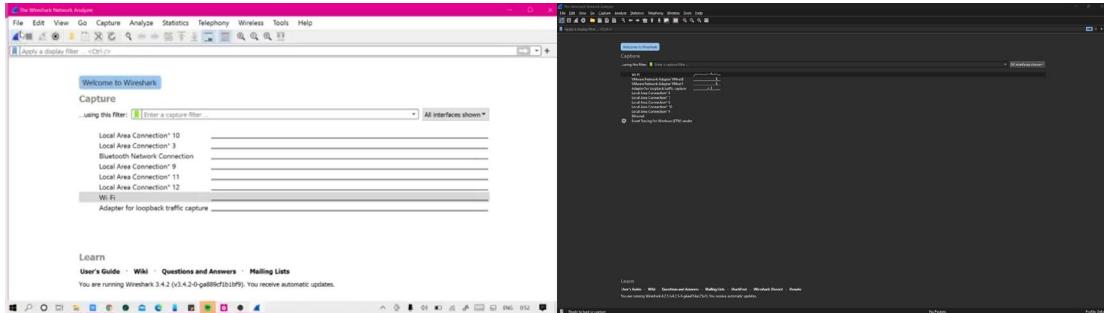
Gambar 2 isntall Wireshark di WIndows 11

Menginstall di desktop Wireshark



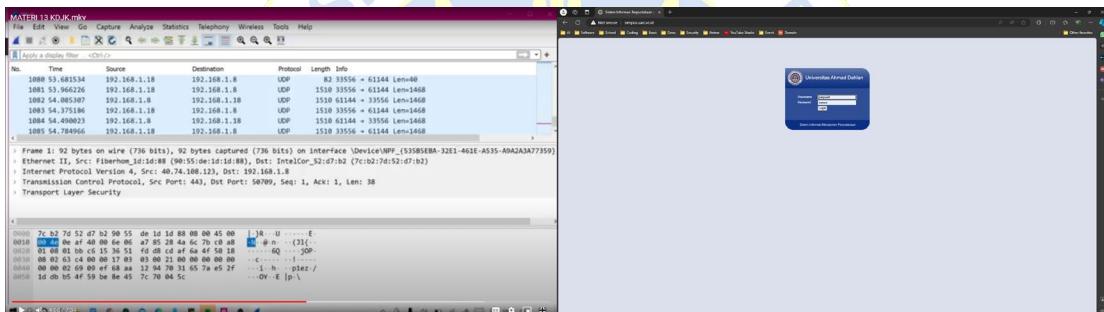
Gambar 3 Shortcut Wireshark di startmenu

Program Wireshark berhasil di install



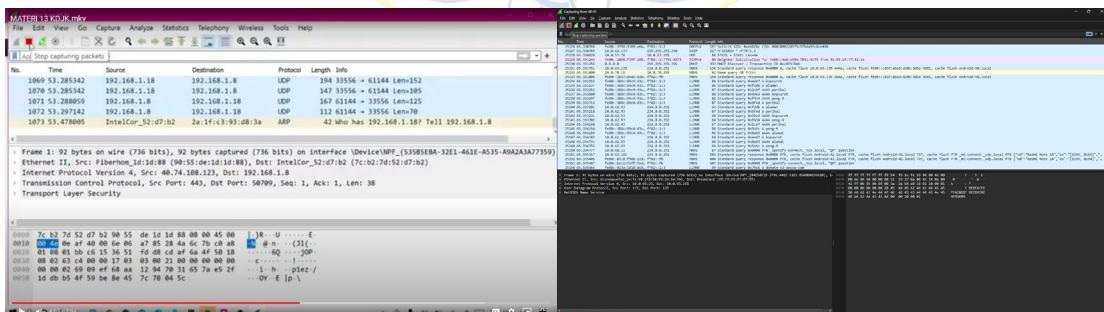
Gambar 4 Menekan icon shark di kiri atas untuk start capturing

Mencoba capturing dari tif.uad.ac.id, karena website ini sudah lampau dan tidak ada login, maka aku akan mencoba capturing dengan http://simpus.uad.ac.id/



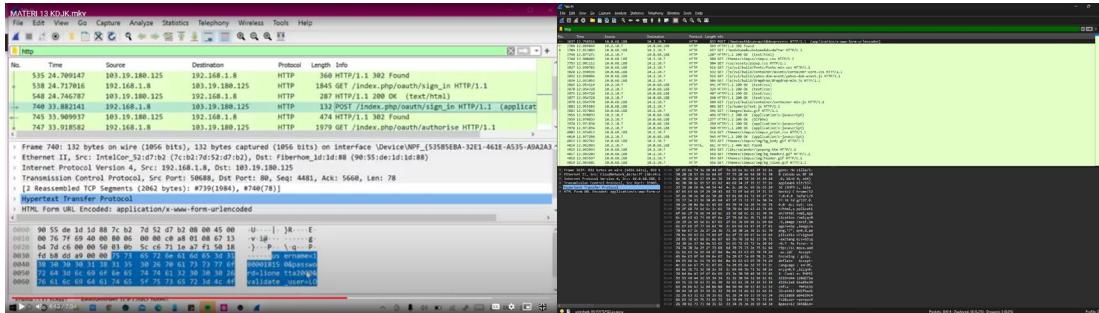
Gambar 5 Mencoba login di simpus.uad.ac.id

Dan setelah login



Gambar 6 Stop capture

Kita stop capture dengan ikon kotak berwarna merah



Gambar 7 Filtering web http

Kita coba ketik http



Gambar 8 mencari http di search bar untuk filter pencarian

Dan searching bagian post

No.	Time	Source	Destination	Protocol	Length	Info
+	3637 12.758516	10.0.68.188	10.2.10.7	HTTP	832	POST /?mod=auth&sub=auth&do=process HTTP/1.1 (application/x-www-form-urlencoded)

Gambar 9 menemukan POST

Frame 3637: 832 bytes on wire (6656 bits), 832 bytes captured (6656 bits) on interface \Device\NPF_{44E50F33-37B6-44EC-91EC-B60BDB36B28}, id 0
Ethernet II, Src: CloudNetwork_de:6e:7f (60:e9:aa:de:6e:7f), Dst: Cisco_20:f0:f6 (70:6b:b9:20:f0:f6)
Internet Protocol Version 4, Src: 10.0.68.188, C
Transmission Control Protocol, Src Port: 55903, Dst Port: 80
Hypertext Transfer Protocol
POST /?mod=auth&sub=auth&do=process HTTP/1.1 (application/x-www-form-urlencoded)
Content-Type: application/x-www-form-urlencoded
Content-Length: 71
Cache-Control: max-age=0
Origin: http://simpus.uad.ac.id
DNT: 1
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml,application/javascript,application/json
Referer: http://simpus.uad.ac.id
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,id;q=0.8
Cookie: PHPSESSID=e44120d2fbad126c1a86ba84e39
[Full request URI: http://simpus.uad.ac.id/?mod=auth&sub=auth&do=process]
[HTTP request 1/6]
[Response in frame: 3700]
[Next request in frame: 3709]
File Data: 71 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "PHPSESSID" = "e44120d2fbad126c1a86ba84e39"
Form item: "user" = "perpus"
Form item: "pass" = "123456"
Form item: "id" = ""

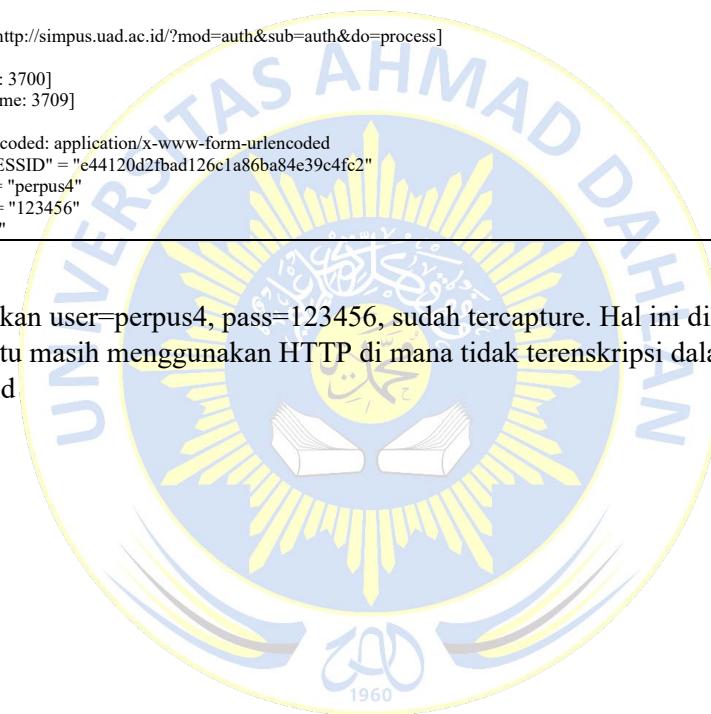
Gambar 10 Terdeteksi POST form yang sudah di input yaitu username dan password

Berikut data yang sudah didapatkan

Frame 3637: 832 bytes on wire (6656 bits), 832 bytes captured (6656 bits) on interface \Device\NPF_{44E50F33-37B6-44EC-91EC-B60BDB36B28}, id 0
Ethernet II, Src: CloudNetwork_de:6e:7f (60:e9:aa:de:6e:7f), Dst: Cisco_20:f0:f6 (70:6b:b9:20:f0:f6)

```
Internet Protocol Version 4, Src: 10.0.68.188, Dst: 10.2.10.7
Transmission Control Protocol, Src Port: 55903, Dst Port: 80, Seq: 1, Ack: 1, Len: 778
Hypertext Transfer Protocol
POST /?mod=auth&sub=auth&do=process HTTP/1.1\r\n
Host: simpus.uad.ac.id\r\n
Connection: keep-alive\r\n
Content-Length: 71\r\n
Cache-Control: max-age=0\r\n
Origin: http://simpus.uad.ac.id\r\n
DNT: 1\r\n
Upgrade-Insecure-Requests: 1\r\n
Content-Type: application/x-www-form-urlencoded\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Edg/127.0.0.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7\r\n
Referer: http://simpus.uad.ac.id/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,id;q=0.8\r\n
Cookie: PHPSESSID=e44120d2fbad126c1a86ba84e39c4fc2\r\n
\r\n
[Full request URI: http://simpus.uad.ac.id/?mod=auth&sub=auth&do=process]
[HTTP request 1/6]
[Response in frame: 3700]
[Next request in frame: 3709]
File Data: 71 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "PHPSESSID" = "e44120d2fbad126c1a86ba84e39c4fc2"
Form item: "user" = "perpus4"
Form item: "pass" = "123456"
Form item: "id" = ""
```

Sudah dimasukkan user="perpus4", pass="123456", sudah tercapture. Hal ini dikarenakan tidak terenkripsi yaitu masih menggunakan HTTP di mana tidak terenkripsi dalam website simpus.uad.ac.id



POST TEST

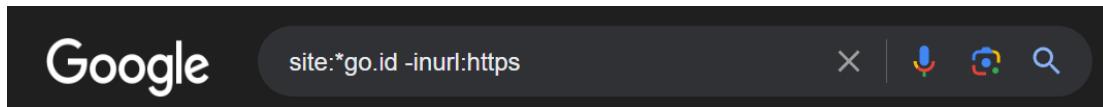
POSTEST:

Lakukan scanning sesuai langkah praktikum dengan 5 website yang berbeda!

Gambar 11 soal post test

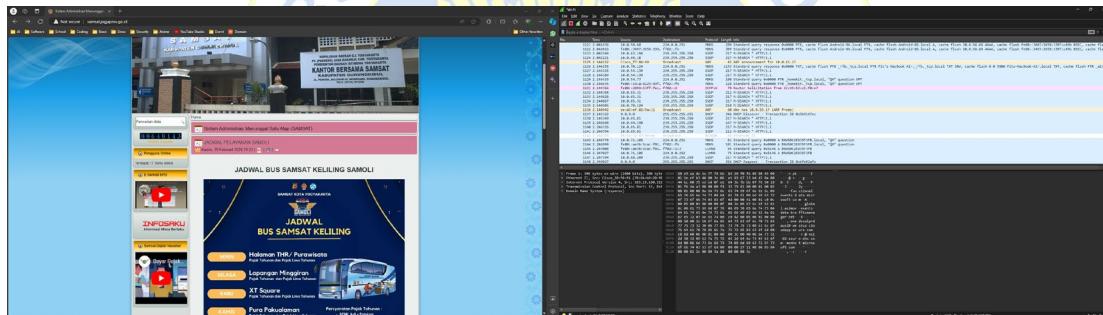
Untuk memudahkan mencari website yang tidak memiliki enkripsi, gunakan keyword berikut dalam Google Search

site:*go.id -inurl:https



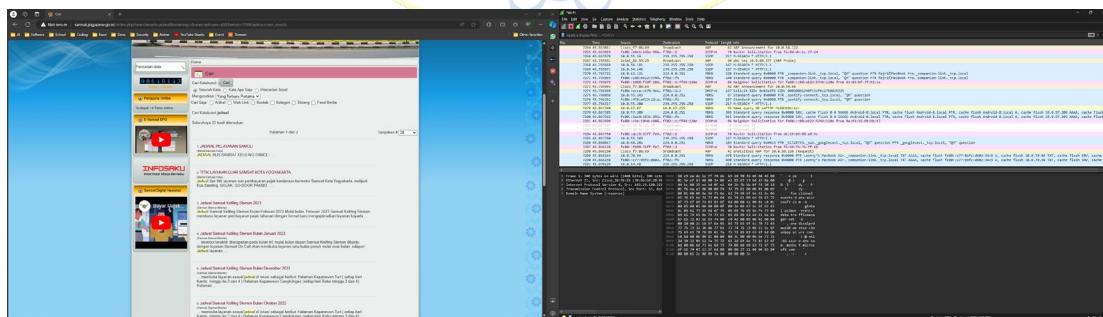
Gambar 12 Mencari kata kunci agar mendapatkan website yang tidak aman

- 1) Spoofing 1: <http://samsat.jogjaprov.go.id/>



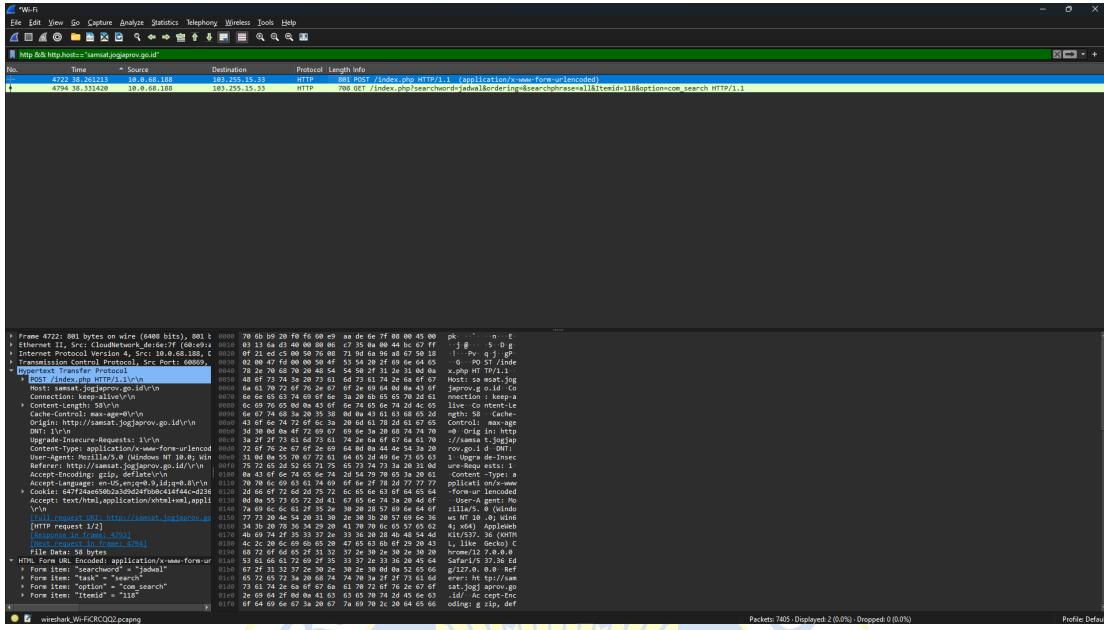
Gambar 13 halaman utama satwsat jogja

Kita coba mencari data, yaitu keyword “jadwal” di searching bawaaan samsat jogjaprov.go.id



Gambar 14 mencari pencarian misalnya searching di halaman tersebut

Setelah melakukan spoofing, kita matikan logging spoofing



Gambar 15 hasil spoofing

Setelah melakukan spoofing dengan Wireshark, dapat terdeteksi di logs Spoofing Wireshark, yaitu searchword dengan jadwal. Hal ini membuat kegiatan user dapat di tracking luas, sehingga dapat membahayakan apabila memasuki hal sensitif di website tersebut walaupun website tersebut di bawah naungan pemerintah .go.id

Berikut adalah data analisis yang dapat di extract,

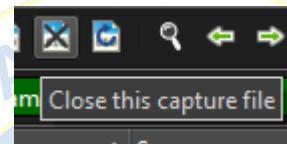
```
Frame 4722: 801 bytes on wire (6408 bits), 801 bytes captured (6408 bits) on interface \Device\NPF_{44E50F33-37B6-44EC-91EC-B60BDB36B28}, id 0
Ethernet II, Src: CloudNetwork_de:6e:7f (60:e9:aa:de:6e:f6), Dst: Cisco_20:f0:f6 (70:6b:b9:20:f0:f6)
Internet Protocol Version 4, Src: 10.0.68.188, Dst: 103.255.15.33
Transmission Control Protocol, Src Port: 60869, Dst Port: 80, Seq: 1, Ack: 1, Len: 747
Hypertext Transfer Protocol
    POST /index.php HTTP/1.1\r\n
    Host: samsat.jogjaprov.go.id\r\n
    Connection: keep-alive\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Content-Length: 58\r\n
    Cache-Control: max-age=0\r\n
    Origin: http://samsat.jogjaprov.go.id\r\n
    DNT: 1\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36 Edg/127.0.0.0\r\n
    Referer: http://samsat.jogjaprov.go.id/\r\n
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,id;q=0.8\r\n
    Cookie: 647f24ae650b2a3d9d24fbb0c414f44c=d2361c006331d0ffda74b3ad0e3a0668\r\n
```

```

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8\r\n
[Full request URI: http://samsat.jogjaprov.go.id/index.php]
[HTTP request 1/2]
[Response in frame: 4793]
[Next request in frame: 4794]
File Data: 58 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "searchword" = "jadwal"
Form item: "task" = "search"
Form item: "option" = "com_search"
Form item: "Itemid" = "118"

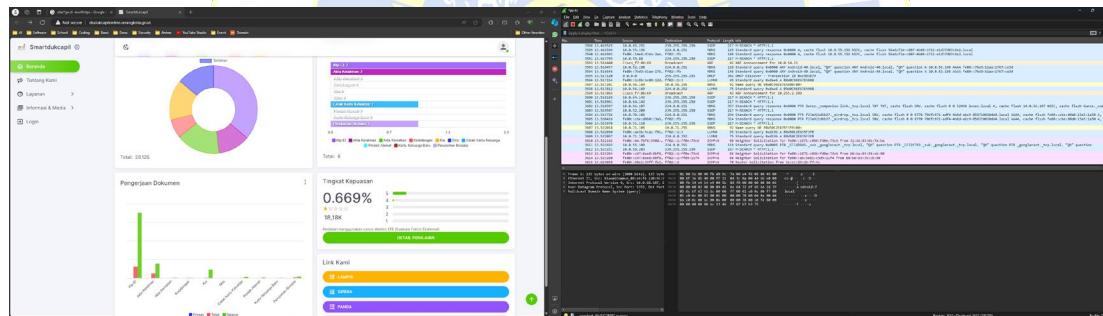
```

Setelah melakukan spoofing dapat melakukan reset logs yaitu dengan emnekan berikut



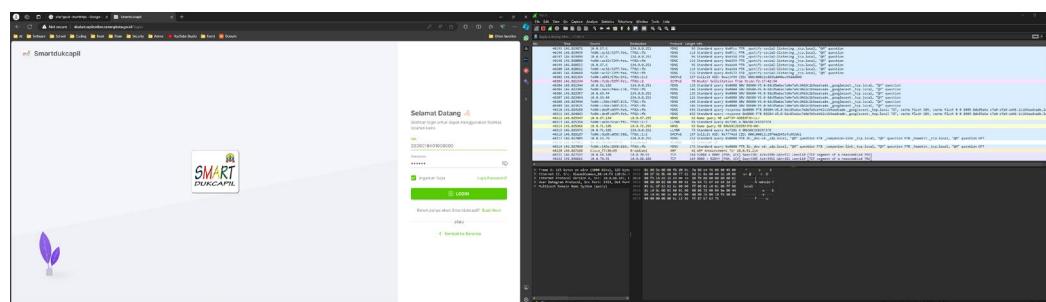
Gambar 16 Close this capture file

2) Spoofing 2: <http://disdukcapilonline.serangkota.go.id/>



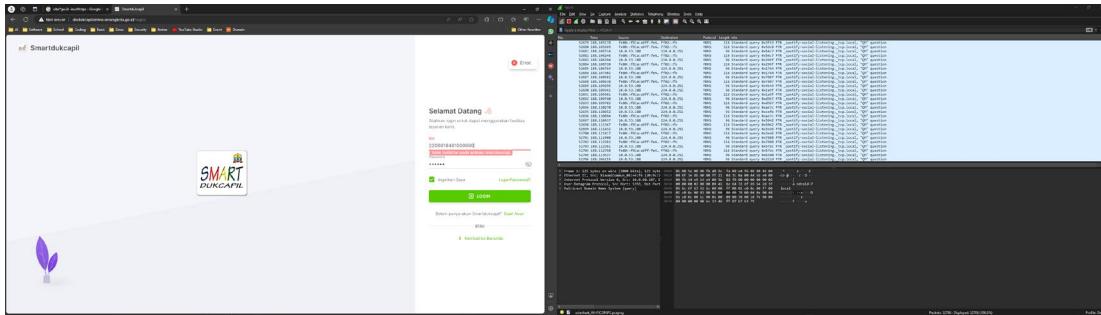
Gambar 17 halaman disdukcapilonline serang kota

Kita masuk halaman utama, setelah itu kita fokus fitur Ikoninya disdukcapilonline di kota Serang



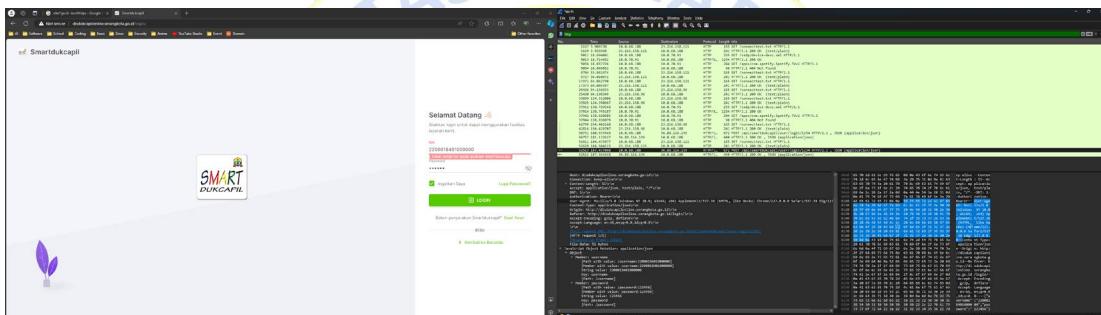
Gambar 18 Masuk ke menu login

Kita masukkan asal dengan nim dan ditambahkan angka tambahan untuk menyesuaikan NIK harus 16 angka dan password yaitu 123456 setelah klik login



Gambar 19 memberhentikan spoofing, dan mengecek login di smartdukcapil

Sekarang kita stop spoofingnya



Gambar 20 data terspoofing disdukcapil

Berikut data yang berhasil di extract,

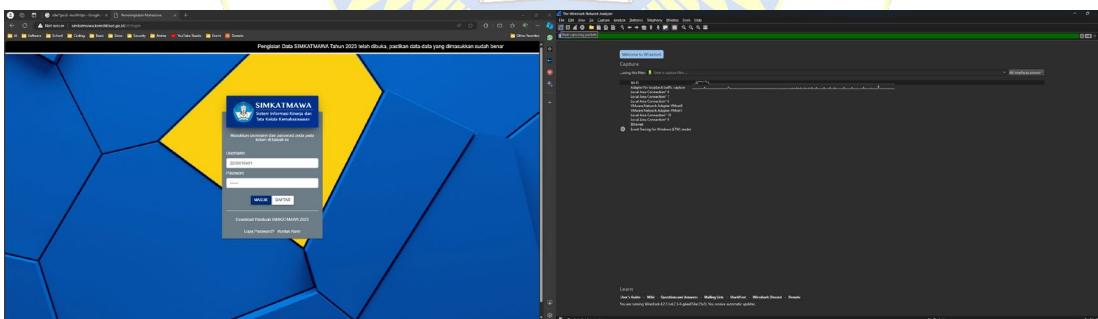
```
Frame 806: 672 bytes on wire (5376 bits), 672 bytes captured (5376 bits) on interface
\Device\NPF_{44E50F33-37B6-44EC-91EC-B60BDB36B28}, id 0
Ethernet II, Src: CloudNetwork_de:6e:7f (60:e9:aa:de:6e:7f), Dst: Cisco_20:f0:f6
(70:6b:b9:20:f0:f6)
Internet Protocol Version 4, Src: 10.0.68.188, Dst: 36.88.116.139
Transmission Control Protocol, Src Port: 63655, Dst Port: 80, Seq: 1, Ack: 1, Len: 618
Hypertext Transfer Protocol
    POST /api/smartdukcapil/user/login/1234 HTTP/1.1\r\n
    Host: disdukcapilonline.serangkota.go.id\r\n
    Connection: keep-alive\r\n
    Content-Length: 51\r\n
    Accept: application/json, text/plain, */*\r\n
    DNT: 1\r\n
    Authorization: Bearer\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36 Edg/127.0.0.0\r\n
    Content-Type: application/json\r\n
    Origin: http://disdukcapilonline.serangkota.go.id\r\n
    Referer: http://disdukcapilonline.serangkota.go.id/login/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,id;q=0.8\r\n
\r\n
```

```
[Full request
http://disdukcapilonline.serangkota.go.id/api/smardukcapil/user/login/1234] URI:
[HTTP request 1/1]
[Response in frame: 827]
File Data: 51 bytes
JavaScript Object Notation: application/json
Object
Member: username
[Path with value: /username:2200018401000000]
[Member with value: username:2200018401000000]
String value: 2200018401000000
Key: username
[Path: /username]
Member: password
[Path with value: /password:123456]
[Member with value: password:123456]
String value: 123456
Key: password
[Path: /password]
```

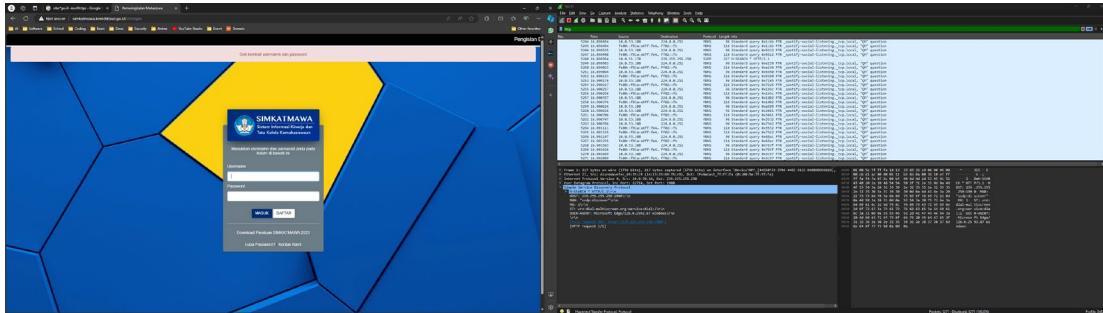
Teryanta, masih bisa dilacak password yang kita masukkan, salah maupun benar (ini contoh yang salah). Hal ini akan merugikan user apabila ada orang pihak ketiga secara tidak berwenang melakukan spoofing untuk kejahatan mendapatkan data user, sekelas pemerintah seperti disdukcapilonline di Kota Serang masih dibilang miris dikarenakan masih menggunakan http sedangkan seharusnya untuk keamanan pengguna yaitu harus di enkripsi

3) Spoofing 3: <http://simkatmawa.kemdikbud.go.id/>

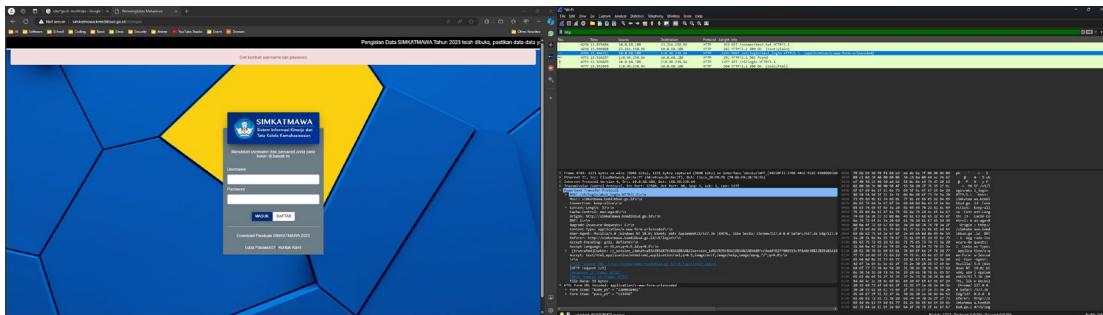
Kita akan mencoba spoofing yang disediakan oleh pemerintah selanjutnya, yaitu kemdikbud



Gambar 21 halaman Simkatmawa



Gambar 22 mencoba login di Simkatmawa



Gambar 23 Berhasil spoofing Simkatmawa

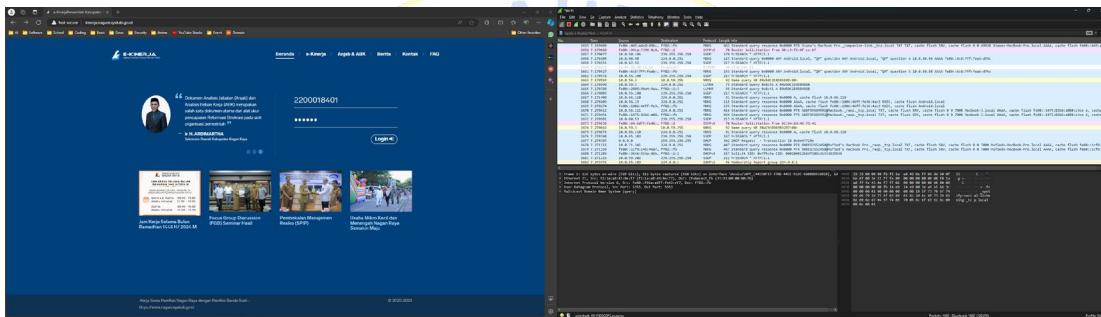
Berikut data yang telah di extract

Frame 4769: 1231 bytes on wire (9848 bits), 1231 bytes captured (9848 bits) on interface \Device\NPF_{44E50F33-37B6-44EC-91EC-B60BDBB36B28}, id 0
 Ethernet II, Src: CloudNetwork_de:6e:7f (60:e9:aa:de:6e:7f), Dst: Cisco_20:f0:f6 (70:6b:b9:20:f0:f6)
 Internet Protocol Version 4, Src: 10.0.68.188, Dst: 118.98.239.64
 Transmission Control Protocol, Src Port: 63509, Dst Port: 80, Seq: 1, Ack: 1, Len: 1177
 Hypertext Transfer Protocol
 POST /v5/login/aksi_login HTTP/1.1\r\n
 Host: simkatmawa.kemdikbud.go.id\r\n
 Connection: keep-alive\r\n
 Content-Length: 33\r\n
 Cache-Control: max-age=0\r\n
 Origin: http://simkatmawa.kemdikbud.go.id\r\n
 DNT: 1\r\n
 Upgrade-Insecure-Requests: 1\r\n
 Content-Type: application/x-www-form-urlencoded\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36 Edg/127.0.0.0\r\n
 Referer: http://simkatmawa.kemdikbud.go.id/v5/login\r\n
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: en-US,en;q=0.9,id;q=0.8\r\n
 [truncated]Cookie:
 ci_session_simkat=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%2289dd8fcc9addf027f906915c3f8e8e30%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A12%3A%22103.19.180.1%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F5.0
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8\r\n
 [Full request URI: http://simkatmawa.kemdikbud.go.id/v5/login/aksi_login]
 [HTTP request 1/2]
 [Response in frame: 4772]
 [Next request in frame: 4773]

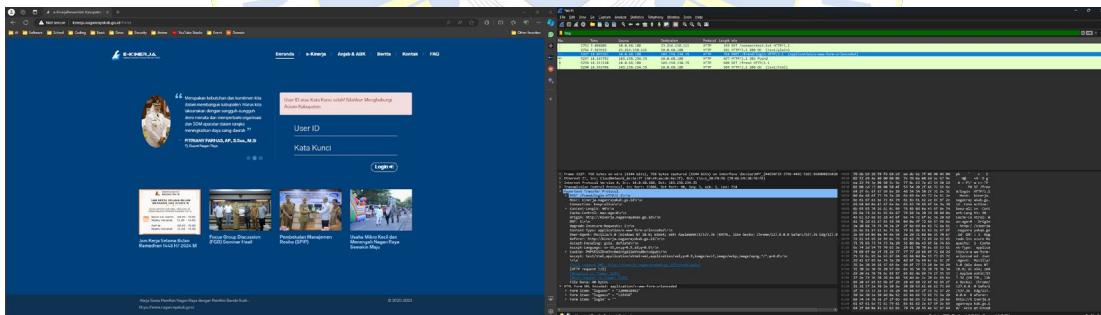
```
File Data: 33 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "kode_pt" = "2200018401"
Form item: "pass_pt" = "123456"
```

Setelah kita analisis, sekelas pemerintah juga yaitu kemdikbud, masih saja tidak menerapkan enkripsi yaitu mengubah dan menambahkan fitur https pada website pemerintah. Hal ini SIMKATMAWA tidak akan dan harus dibenahi lebih lanjut oleh kemdikbud, jika tidak, maka ada pihak yang tidak bertanggung jawab yang melakukan spoofing di mana saja yang dapat membaca kegiatan pengguna.

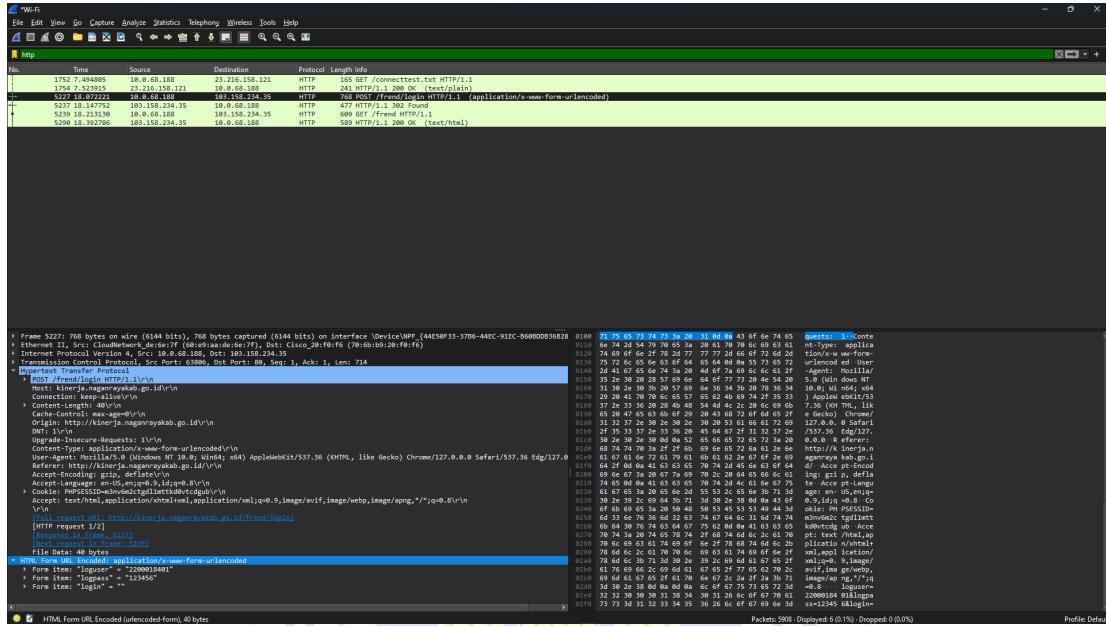
4) Spoofing 4: <http://kinerja.naganrayakab.go.id/>



Gambar 24 Mencoba login di E-Kinerja



Gambar 25 kita coba lihat hasil data spoofing



Gambar 26 Data terdeteksi login, data berhasil di spoofing

Berikut data yang berhasil di extract,

```

Frame 5227: 768 bytes on wire (6144 bits), 768 bytes captured (6144 bits) on interface \Device\NPF_{44E50F33-37B6-44EC-91EC-B60BDB36B28}, id 0
Ethernet II, Src: CloudNetwork_de:6e:7f (60:e9:aa:de:6e:7f), Dst: Cisco_20:f0:f6 (70:6b:b9:20:f0:f6)
Internet Protocol Version 4, Src: 10.0.68.188, Dst: 103.158.234.35
Transmission Control Protocol, Src Port: 63806, Dst Port: 80, Seq: 1, Ack: 1, Len: 714
Hypertext Transfer Protocol
POST /frend/login HTTP/1.1\r\n
Host: kinerja.naganrayakab.go.id\r\n
Connection: keep-alive\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Cache-Control: max-age=0\r\n
Origin: http://kinerja.naganrayakab.go.id\r\n
DNT: 1\r\n
Upgrade-Insecure-Requests: 1\r\n
Content-Type: application/x-www-form-urlencoded\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/1537.36 Edg/127.0\r\n
Referer: http://kinerja.naganrayakab.go.id/\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.9,id;q=0.8\r\n
Cookie: PHPSESSID=m3nv6m2ctgd1lmttkd0vtcdgub\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8\r\n
\r\n
[Full request URI: http://kinerja.naganrayakab.go.id/frend/login]
[HTTP request 1/2]
[Response in frame: 5237]
[Next request in frame: 5239]
File Data: 40 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "loguser" = "2200018401"
Form item: "logpass" = "123456"
Form item: "login" = ""

```

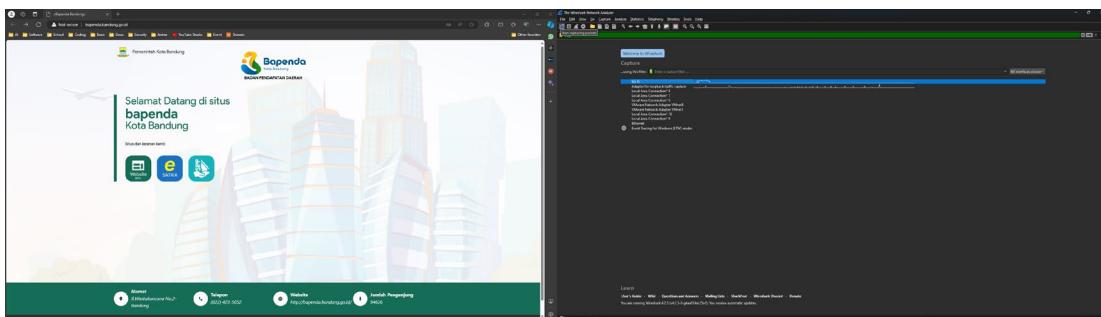
Disini terlihat loguser dan logpass dikarrenakan tidak menggunakan transport yang terenskripsi. Hal ini akan membahayakan pengguna apabila login ke website E-Kinerja sehingga harus sigap dibenahi oleh pemerintah kabupaten Naganraya.

Setelah dicek lanjut, ternyata ada website serupa membahas tentang e-Kinerja seperti,

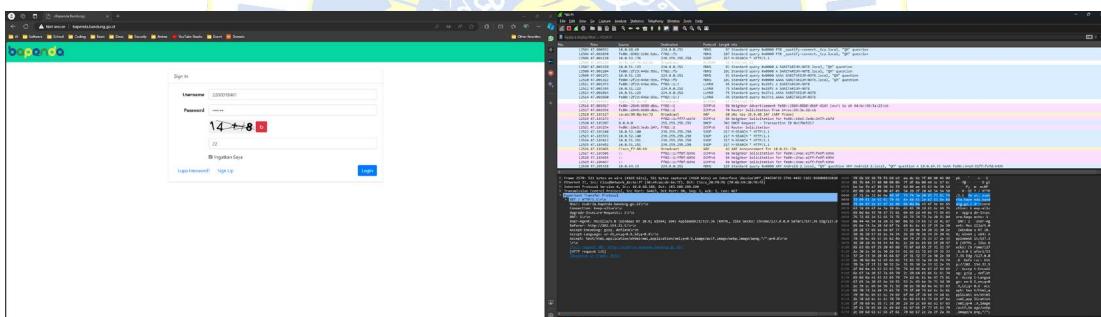
<http://kinerja.acehbaratdayakab.go.id/>

juga tidak menggunakan enskripsi.

5) Spoofing 5: <http://bapenda.bandung.go.id/>

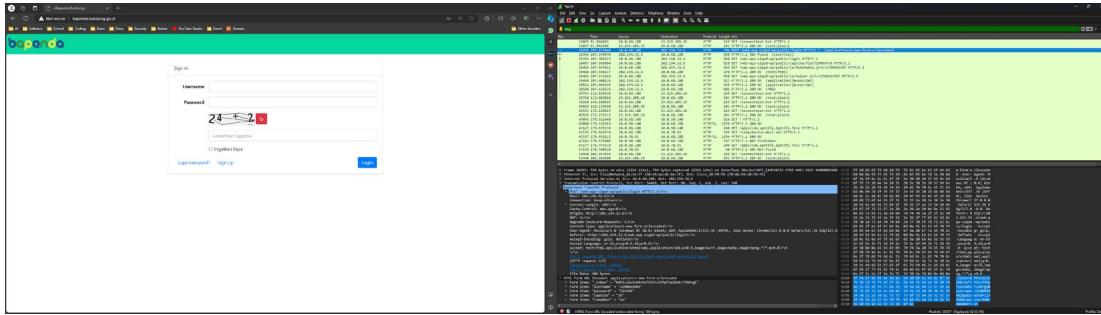


Gambar 27 Halaman utama Bapenda bandung



Gambar 28 Mencoba login dan memasukkan captcha

Disini menerapkan captcha, hal keunikan website login lainnya untuk mencegah boot, mari kita coba login



Gambar 29 Capture hasil login di Bapeda Bandung

Berikut data extract yang didapatkan,

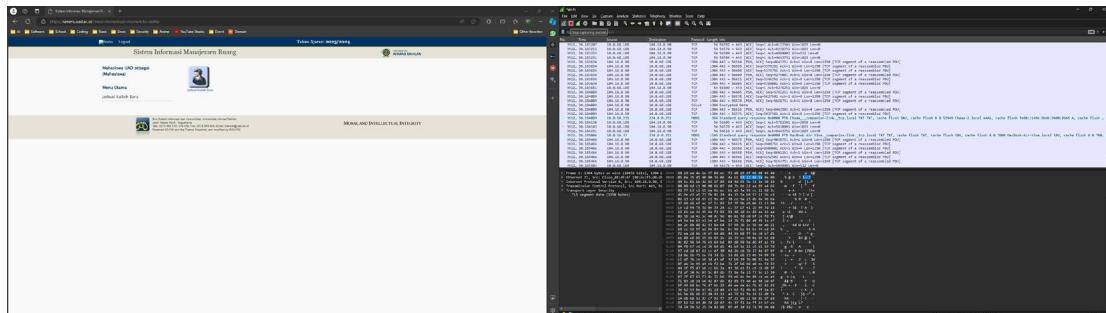
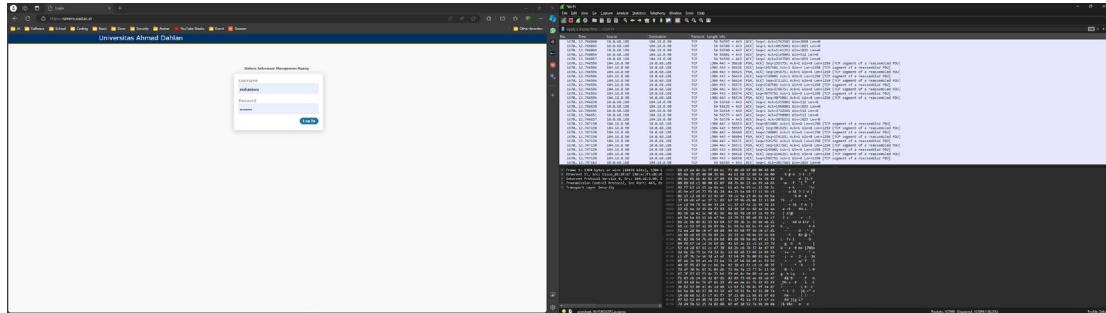
```

Frame 28265: 794 bytes on wire (6352 bits), 794 bytes captured (6352 bits) on interface
\Device\NPF_{44E50F33-37B6-44EC-91EC-B60BDB36B28}, id 0
Ethernet II, Src: CloudNetwork_de:6e:7f (60:e9:aa:de:e6:f6),
(Dst: Cisco_20:f0:f6
(70:6b:b9:20:f0:f6)
Internet Protocol Version 4, Src: 10.0.68.188, Dst: 202.154.32.6
Transmission Control Protocol, Src Port: 64469, Dst Port: 80, Seq: 1, Ack: 1, Len: 740
Hypertext Transfer Protocol
    POST /web-app-sippd-wp/public/login HTTP/1.1\r\n
    Host: 202.154.32.6\r\n
    Connection: keep-alive\r\n
    Content-Length: 106\r\n
    Cache-Control: max-age=0\r\n
    Origin: http://202.154.32.6\r\n
    DNT: 1\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36 Edg/127.0.0.0\r\n
    Referer: http://202.154.32.6/web-app-sippd-wp/public/login\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,id;q=0.8\r\n
    Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8\r\n
\r\n
[Full request URI: http://202.154.32.6/web-app-sippd-wp/public/login]
[HTTP request 1/3]
[Response in frame: 28354]
[Next request in frame: 28355]
File Data: 106 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "_token" = "kMPiLAlo2u9Bvto71YS1cJ5Ppf1eIUwkvTZAHrgi"
Form item: "username" = "2200018401"
Form item: "password" = "123456"
Form item: "captcha" = "36"
Form item: "remember" = "on"

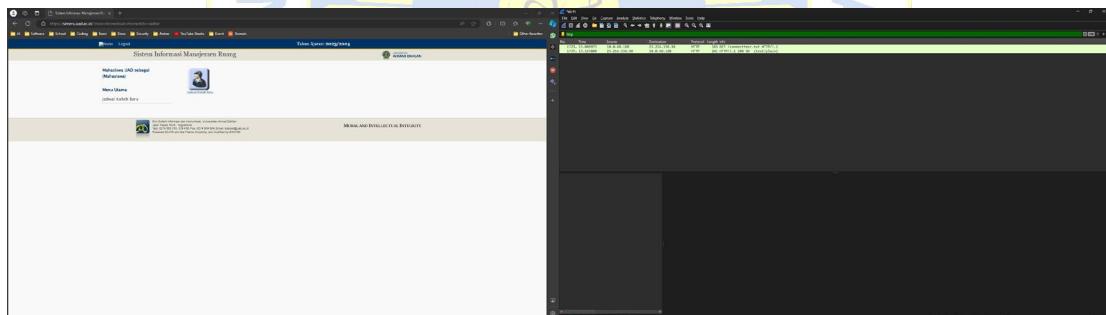
```

Sekelas Badan Pendapatan Daerah (BAPENDA) masih saja tidak dienskripsi, padahal ini sangat krusial yaitu tentang pendapatan keuangan di daerah yaitu di Bandung. Hal ini akan membuat resiko terkena hacking dan diobrak abrik oleh pihak yang tidak berwernang. Disarankan pemerintah menggunakan enskripsi yang memadai.

- 6) Spoofing HTTPS (Bonus): <https://simeru.uad.ac.id/>



Kita filtering http



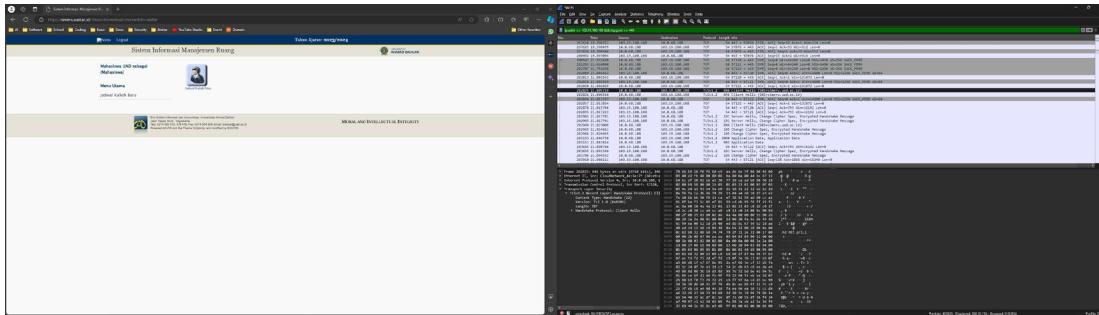
Tidak ada yang cocok, karena ini menggunakan https, oleh karena itu kita menggunakan filtering berdasarkan tcp yaitu Filter `tcp.port==443` dan ip address website

```
C:\Users\ireddragonicy>nslookup simeru.uad.ac.id
Server:  UnKnown
Address: 103.19.180.211

Non-authoritative answer:
Name:    simeru.uad.ac.id
Address: 103.19.180.108
```

Sehingga filteringnya adalah

```
ip.addr == 103.19.180.108 && tcp.port == 443
```



Ternyata terenkripsi, sehingga data yang terlihat aman dan tidak dapat dispooffing orang lain, di dalam website simeru.uad.ac.id karena menggunakan https.

Kesimpulan:

Berdasarkan hasil praktikum yang saya kerjakan, menunjukkan dengan jelas perbedaan keamanan antara protokol HTTP dan HTTPS. Website yang masih menggunakan HTTP sangat rentan terhadap serangan man-in-the-middle dan packet sniffing. Data sensitif seperti username dan password dapat dengan mudah tertangkap dan dibaca oleh pihak ketiga yang tidak berwenang. Sebaliknya, website yang menggunakan HTTPS (seperti simeru.uad.ac.id) menunjukkan tingkat keamanan yang jauh lebih tinggi, di mana data yang ditransmisikan terenkripsi dan tidak dapat dibaca meskipun berhasil ditangkap.

Sangat mengkhawatirkan bahwa banyak website pemerintah dan lembaga publik masih menggunakan protokol HTTP yang tidak aman. Ini termasuk website-website kritis seperti:

- Sistem Informasi Kependudukan dan Pencatatan Sipil (<http://disdukcapilonline.serangkota.go.id/>)
- Sistem Informasi Kegiatan Mahasiswa (<http://simkatmawa.kemdikbud.go.id/>)
- Sistem Kinerja Pemerintah Daerah (<http://kinerja.naganrayakab.go.id/>)
- Badan Pendapatan Daerah (<http://bapenda.bandung.go.id/>) Kerentanan ini membuka peluang besar untuk peretasan data dan penyalahgunaan informasi warga negara.

Terlihat juga betapa mudahnya informasi sensitif seperti NIK, username, dan password dapat diintercept ketika ditransmisikan melalui jaringan yang tidak aman. Ini menimbulkan risiko serius terhadap privasi dan keamanan data pribadi warga negara.

Hal ini harus didorong kebutuhan mendesak bagi pemerintah dan institusi publik untuk meningkatkan keamanan sistem informasi mereka. Migrasi dari HTTP ke HTTPS harus menjadi prioritas utama untuk melindungi data warga negara dan integritas sistem pemerintahan. Intinya, **ganti SDM PEMERINTAH >:V**