

**Tugas Keamanan Jaringan Komputer tapping password menggunakan  
wireshark, Tor dan John The Ripper**

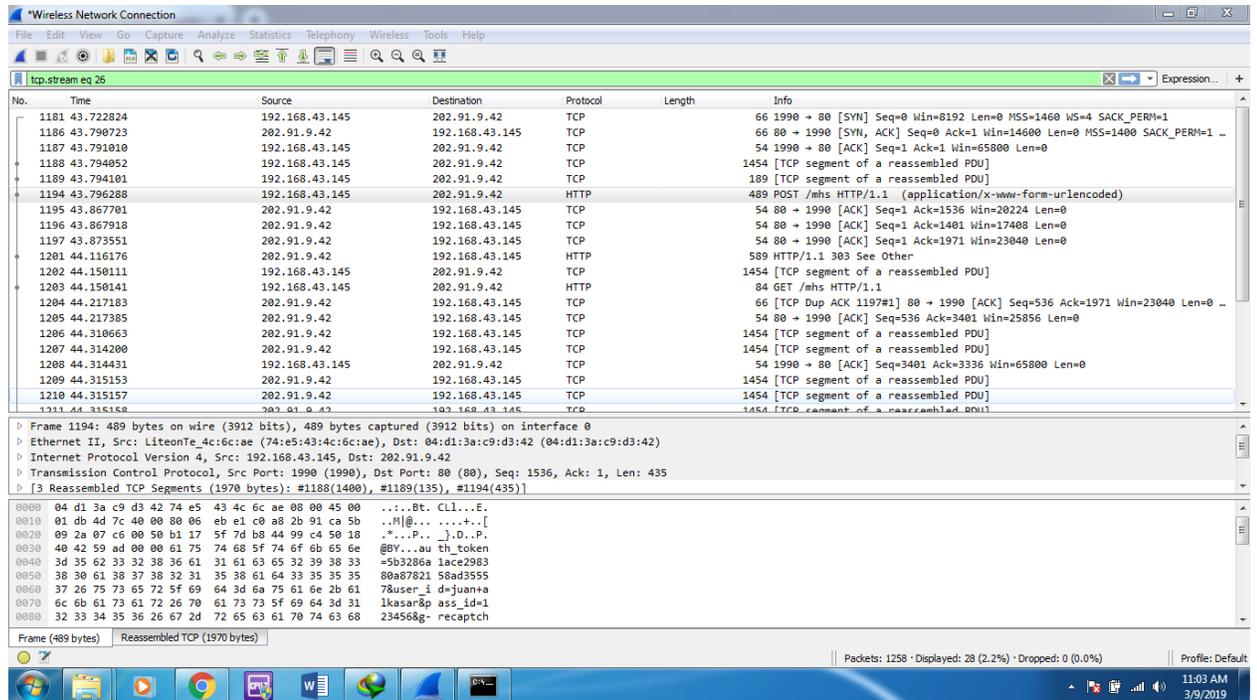


Oleh :  
**JUAN ALKASAR**  
**09011281520092**

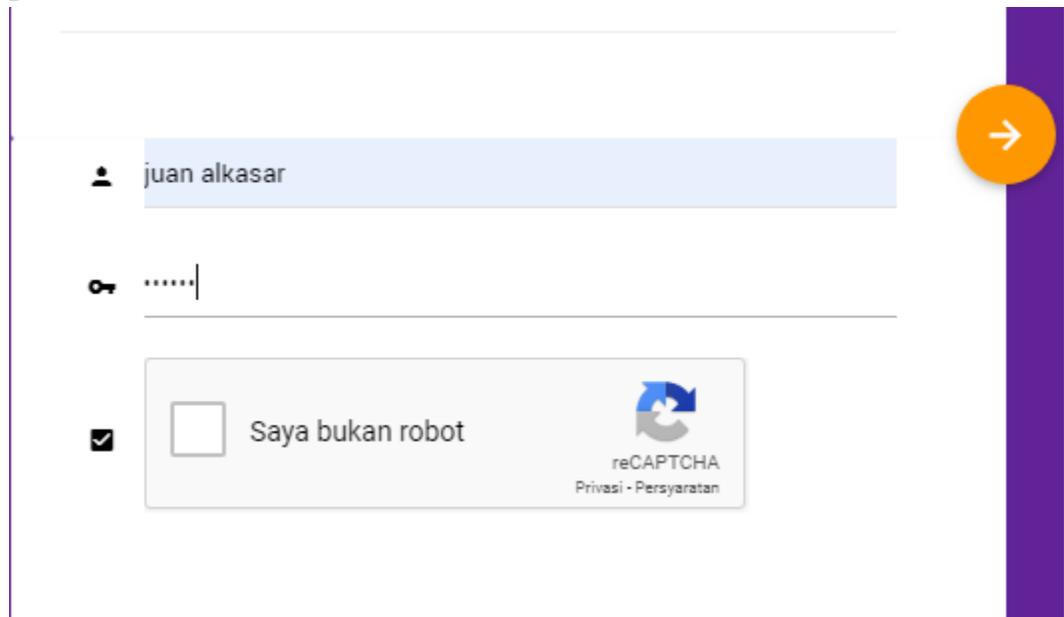
**Jurusan Sistem Komputer**  
**Fakultas Ilmu Komputer**  
**Universitas Sriwijaya**  
**2019**

# 1. Taping password kamu sendiri (menggunakan tools wireshark)

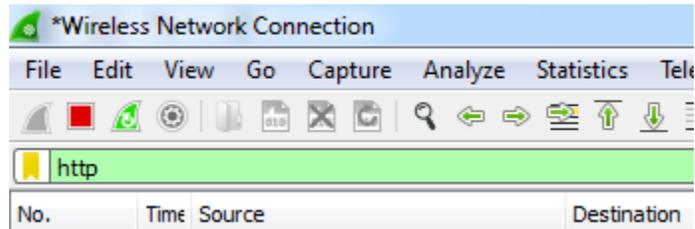
- Langkah pertama adalah kita membuka aplikasi wireshark.



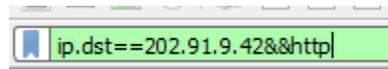
- Kemudian kita membuka website yang ingin kita buka atau kita lihat password kita sendiri.



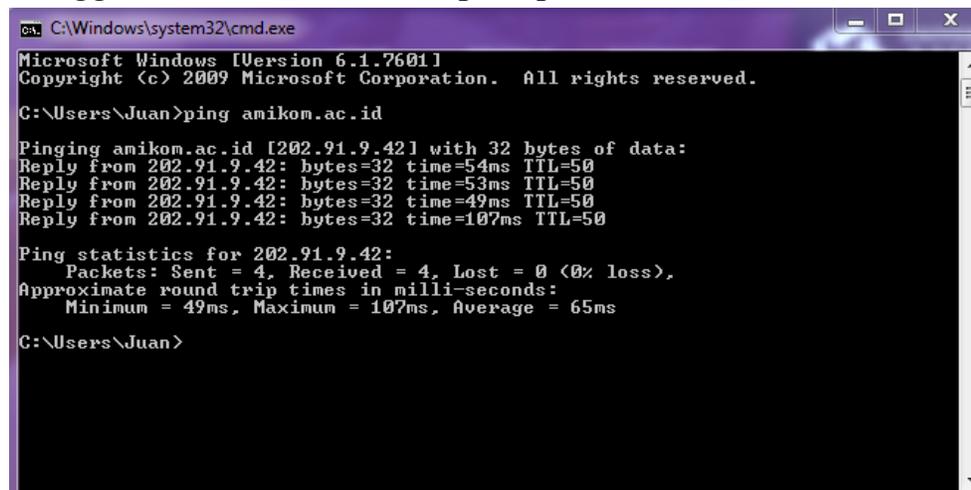
- Pada tampilan wireshark kita filter bagian http, disini saya menggunakan login tanpa menggunakan https.



- Bisa juga dengan menggunakan command dibawah ini.



- Untuk mengetahui ip dari website yang kita gunakan kita bisa menggunakan cmd(command prompt).



- Pada bagian http kita cari dibagian info ada kata login.
- Kemudian kita pilih, dan klik kanan pada bagian http
- Pilih follow, akan muncul lagi beberapa pilihan
- Pilih TCP stream

- Kemudian akan muncul tampilan seperti gambar dibawah ini, gambar dibawah ini menunjukkan username dan password yang telah kita gunakan pada suatu website.

```
Wireshark · Follow TCP Stream (tcp.stream eq 26) · wireshark_pcapng_77568f29-4822-4f29-8144-90f551e52e3b_20190309105814_a01148

POST /mhs HTTP/1.1
Host: auth.amikom.ac.id
Connection: keep-alive
Content-Length: 435
Cache-Control: max-age=0
Origin: http://auth.amikom.ac.id
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://auth.amikom.ac.id/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,id;q=0.8
Cookie: __utma=104080735.1695834135.1552099830.1552099830.1552099830.1;
__utmz=104080735.1552099830.1.1.utmcsr=amikom.ac.id|utmccn=(referral)|utmcmd=referral|utmcct=/; ci_session=a%3A4%3A%7B%
%3A10%3A%22session_id%22%3B%3A32%3A%22edf2527d14d0ad20a029b9db058e964a%22%3B%3A10%3A%22ip_address%22%3B%3A12%3A
%22116.206.35.3%22%3B%3A10%3A%22user_agent%22%3B%3A50%3A%22Mozilla%2F5.0+%28Windows+NT+6.1%29+AppleWebKit%2F537.36+%28K
%22%3B%3A13%3A%22last_activity%22%3B%3A10%3A%221552103318%22%3B%3A70e629a7809b16ef914903ab1050265415;
rtauth_cookie=5b3286a1ace298380a8782158ad35557; rtamikom=a%3A4%3A%7B%3A10%3A%22session_id%22%3B%3A32%3A
%2219db5d0ac7fe116bd19f71fb0cf785b5%22%3B%3A10%3A%22ip_address%22%3B%3A12%3A%22116.206.35.3%22%3B%3A10%3A%22user_agent
%22%3B%3A50%3A%22Mozilla%2F5.0+%28Windows+NT+6.1%29+AppleWebKit%2F537.36+%28K%22%3B%3A13%3A%22last_activity%22%3B%
%3A10%3A%221552103900%22%3B%3A7Dea81b1a9f56c0407671194449ebb4880; amikom=833856fe0fa7e6250fe1aed2530b68c53e238c23

auth_token=5b3286a1ace298380a8782158ad35557&user_id=juan+alkasar&pass_id=123456&g-recaptcha-
response=03AOLTLQoIKPk2jvrv9eBMTWp_bjlyixIPnD97Cp1-
_K6sud_OCpcJDjgQjgMfMnTmWky9_0k2dzrPZBTcw07H0X5BxKQ5jbyskFB1_oxB5dSDKcg7KfpzSxCSb5ITd-
XUBxp62sqPRndR07fbYbtAhm0LtnecKLD_TitfQj18W0-Ikq0t9063Fg-trbdfbaV9Rz2HnpN2o7FftFZSsExAc1b_Jmqls-Upp-
K6p6gKCSJfSIT_fazbMv5NZuWsbth7bqZuNd376dvFqzDfajX39MtwyIKQDz2db1sVex0aBTL_B2qnYR_6LkTX0hiHtHtoevz7wreaCTHTTP/1.1 303 See
Other
Date: Sat, 09 Mar 2019 03:58:56 GMT
Server: Apache
X-Powered-By: PHP/5.4.41
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: rtauth_cookie=5b3286a1ace298380a8782158ad35557; expires=Sat, 09-Mar-2019 04:58:56 GMT; path=/;
domain=amikom.ac.id; httponly
Location: http://auth.amikom.ac.id/mhs
Content-Length: 0

Packet 1188. 5 client pkt(s). 9 server pkt(s). 3 turns. Click to select.
```

```
Wireshark · Follow TCP Stream (tcp.stream eq 26) · wireshark_pcapng_77568f29-4822-4f29-8144-90f551e52e3b_20190309105814_a01148

POST /mhs HTTP/1.1
Host: auth.amikom.ac.id
Connection: keep-alive
Content-Length: 435
Cache-Control: max-age=0
Origin: http://auth.amikom.ac.id
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://auth.amikom.ac.id/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,id;q=0.8
Cookie: __utma=104080735.1695834135.1552099830.1552099830.1552099830.1;
__utmz=104080735.1552099830.1.1.utmcsr=amikom.ac.id|utmccn=(referral)|utmcmd=referral|utmcct=/; ci_session=a%3A4%3A%7B%
%3A10%3A%22session_id%22%3B%3A32%3A%22edf2527d14d0ad20a029b9db058e964a%22%3B%3A10%3A%22ip_address%22%3B%3A12%3A
%22116.206.35.3%22%3B%3A10%3A%22user_agent%22%3B%3A50%3A%22Mozilla%2F5.0+%28Windows+NT+6.1%29+AppleWebKit%2F537.36+%28K
%22%3B%3A13%3A%22last_activity%22%3B%3A10%3A%221552103318%22%3B%3A70e629a7809b16ef914903ab1050265415;
rtauth_cookie=5b3286a1ace298380a8782158ad35557; rtamikom=a%3A4%3A%7B%3A10%3A%22session_id%22%3B%3A32%3A
%2219db5d0ac7fe116bd19f71fb0cf785b5%22%3B%3A10%3A%22ip_address%22%3B%3A12%3A%22116.206.35.3%22%3B%3A10%3A%22user_agent
%22%3B%3A50%3A%22Mozilla%2F5.0+%28Windows+NT+6.1%29+AppleWebKit%2F537.36+%28K%22%3B%3A13%3A%22last_activity%22%3B%
%3A10%3A%221552103900%22%3B%3A7Dea81b1a9f56c0407671194449ebb4880; amikom=833856fe0fa7e6250fe1aed2530b68c53e238c23

auth_token=5b3286a1ace298380a8782158ad35557&user_id=juan+alkasar&pass_id=123456&g-recaptcha-
response=03AOLTLQoIKPk2jvrv9eBMTWp_bjlyixIPnD97Cp1-
_K6sud_OCpcJDjgQjgMfMnTmWky9_0k2dzrPZBTcw07H0X5BxKQ5jbyskFB1_oxB5dSDKcg7KfpzSxCSb5ITd-
XUBxp62sqPRndR07fbYbtAhm0LtnecKLD_TitfQj18W0-Ikq0t9063Fg-trbdfbaV9Rz2HnpN2o7FftFZSsExAc1b_Jmqls-Upp-
K6p6gKCSJfSIT_fazbMv5NZuWsbth7bqZuNd376dvFqzDfajX39MtwyIKQDz2db1sVex0aBTL_B2qnYR_6LkTX0hiHtHtoevz7wreaCTHTTP/1.1 303 See
Other
Date: Sat, 09 Mar 2019 03:58:56 GMT
Server: Apache
X-Powered-By: PHP/5.4.41
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: rtauth_cookie=5b3286a1ace298380a8782158ad35557; expires=Sat, 09-Mar-2019 04:58:56 GMT; path=/;
domain=amikom.ac.id; httponly
Location: http://auth.amikom.ac.id/mhs
Content-Length: 0

5 client pkt(s). 9 server pkt(s). 3 turns.

Entire conversation (12 kB) Show data as ASCII Stream 26
Find: pass_id=123456 Find Next
```

- Bisa kita lihat username dan password yang kita gunakan sebelumnya

```
POST /ucp.php?mode=login&sid=fd39333bed9917d88fb76365e0d9bc87 HTTP/1.1
Host: forum.cyclingnews.com
Connection: keep-alive
Content-Length: 125
Cache-Control: max-age=0
Origin: http://forum.cyclingnews.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://forum.cyclingnews.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,id;q=0.8
Cookie: cynforum_u=1; cynforum_k=; cynforum_sid=fd39333bed9917d88fb76365e0d9bc87; _ga=GA1.2.1808824941.1552134951; _gid=GA1.2.1331425554.1552134951; _gat=1; _cmpQcif3pcsupported=1; _fbp=fb.1.1552134954224.588013024

username=juanalkasar&password=123456&login=Login&autologin=on&redirect=.%2Findex.php%3Fsid%3Dfd39333bed9917d88fb76365e0d9bc87HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 09 Mar 2019 12:35:55 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: private, no-cache="set-cookie"
Expires: 0
Pragma: no-cache
Content-Encoding: gzip

172e
.....\yw.F.....[. . . . . B.by.I.$..3v....dm...4IH.....).....II.v./.....z|....lvd!
{.....cf.....c.yr...../X...^Y...Y..H.....w.K..s.sEP..M.....A..0..
+.wwwE?.A6.."X.....c{...../.&w..}.....&R.6.s.\-/-...v.H.....*U.....Y.....g.....(/!_.....swj."'.v.
B."I...Z.3...<.g.....#.aU.?.%.....a2v...x.eA.h."..1.....X.....=K.y.
.4I. c.....Y0 <.....9?.....x2.(8.."..s..'..dl.....b.z. '$'.A...@.for...c.B.....2..Gv....G.n...
.E...S..w.bc.....Qm...=/b...7...s.....W.../..vN..w...;.....Yn..`M..9..
.....V.k...O...<.....w.u.n.m.(~..W...{E..0...f.....C T...?E.....?}.....|v.....+.....-x.....q<<
9.aj.tk. |.V.t.$?Z...h.v.....qG.....0..8..$.m.n .S.)].....\V.%..b.n...:U0g9Z.N.V"...m.2.1.ouY.
2...b.9.!...l...Azsh...h{..A/.y.4..<.[
.n..K.kfPR6.h'.....v.....l.....&?.....A..7.....4.K

Packet 1473: 1 client pkt(s), 5 server pkt(s), 1 turn. Click to select.
```

```
POST /ucp.php?mode=login&sid=fd39333bed9917d88fb76365e0d9bc87 HTTP/1.1
Host: forum.cyclingnews.com
Connection: keep-alive
Content-Length: 125
Cache-Control: max-age=0
Origin: http://forum.cyclingnews.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://forum.cyclingnews.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,id;q=0.8
Cookie: cynforum_u=1; cynforum_k=; cynforum_sid=fd39333bed9917d88fb76365e0d9bc87; _ga=GA1.2.1808824941.1552134951; _gid=GA1.2.1331425554.1552134951; _gat=1; _cmpQcif3pcsupported=1; _fbp=fb.1.1552134954224.588013024

username=juanalkasar&password=123456&login=Login&autologin=on&redirect=.%2Findex.php%3Fsid%3Dfd39333bed9917d88fb76365e0d9bc87HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 09 Mar 2019 12:35:55 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: private, no-cache="set-cookie"
Expires: 0
Pragma: no-cache
Content-Encoding: gzip

172e
.....\yw.F.....[. . . . . B.by.I.$..3v....dm...4IH.....).....II.v./.....z|....lvd!
{.....cf.....c.yr...../X...^Y...Y..H.....w.K..s.sEP..M.....A..0..
+.wwwE?.A6.."X.....c{...../.&w..}.....&R.6.s.\-/-...v.H.....*U.....Y.....g.....(/!_.....swj."'.v.
B."I...Z.3...<.g.....#.aU.?.%.....a2v...x.eA.h."..1.....X.....=K.y.
.4I. c.....Y0 <.....9?.....x2.(8.."..s..'..dl.....b.z. '$'.A...@.for...c.B.....2..Gv....G.n...
.E...S..w.bc.....Qm...=/b...7...s.....W.../..vN..w...;.....Yn..`M..9..
.....V.k...O...<.....w.u.n.m.(~..W...{E..0...f.....C T...?E.....?}.....|v.....+.....-x.....q<<
9.aj.tk. |.V.t.$?Z...h.v.....qG.....0..8..$.m.n .S.)].....\V.%..b.n...:U0g9Z.N.V"...m.2.1.ouY.
2...b.9.!...l...Azsh...h{..A/.y.4..<.[
.n..K.kfPR6.h'.....v.....l.....&?.....A..7.....4.K

1 client pkt(s), 5 server pkt(s), 1 turn.
```

## 2. Taping menggunakan tool TOR

This page is also available in the following languages: English



**Congratulations. This browser is configured to use Tor.**

Your IP address appears to be: **89.31.57.5**

Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: [Relay Search](#).

[Donate to Support Tor](#)

[Tor Q&A Site](#) | [Volunteer](#) | [Run a Relay](#) | [Stay Anonymous](#)



- Tapping menggunakan wireshark  
<http://www.kemdikbud.go.id/> ip address 118.98.227.101

The screenshot shows a web browser window displaying the website of the Indonesian Ministry of Education and Culture (Kemendikbud). The browser address bar shows the URL <https://www.kemdikbud.go.id>. The website content includes the ministry logo, navigation tabs (ePPID, Siswa, Guru, Orang Tua, Sekolah, Budaya dan Bahasa, Masyarakat dan Mitra, Peme Dae), and a 'Layanan' (Services) section with various information links.

Overlaid on the bottom of the browser window is the Wireshark network traffic capture window. The filter is set to `ip.dst==118.98.227.101`. The capture shows four ICMP Echo (ping) request packets from source IP 192.168.43.145 to destination IP 118.98.227.101. The packets are numbered 14432, 14439, 14442, and 14445.

No.	Time	Source	Destination	Protocol	Length	Info
14432	9...	192.168.43.145	118.98.227.101	ICMP	74	Echo (ping) request id=0x0001, seq=5/128...
14439	1...	192.168.43.145	118.98.227.101	ICMP	74	Echo (ping) request id=0x0001, seq=6/153...
14442	1...	192.168.43.145	118.98.227.101	ICMP	74	Echo (ping) request id=0x0001, seq=7/179...
14445	1...	192.168.43.145	118.98.227.101	ICMP	74	Echo (ping) request id=0x0001, seq=8/204...

<http://www.palembang.go.id/> ip address 182.23.103.155

The image shows a screenshot of a web browser displaying the official website of Palembang City Government (www.palembang.go.id). The website features a navigation menu on the left with items: BERANDA, TENTANG PALEMBANG, PEMERINTAH KOTA, WEBMAIL, GALERI FOTO, AGENDA WALKOTA, and PENGADUAN MASYARAKAT. The main content area includes a search bar, a "PETA" button, and a "MARI KITA SU" banner. Below the banner is a large image of the "Tugu Selido" monument. To the right, there is an "AGENDA WALKOTA" section with a calendar view showing events for January 11th and 12th, including "shalat shubuh berjamaah bersama Walikota Palembang" and "Pembukaan Bimbingan Teknis Wirausaha Raru IKM".

Below the browser window, a Wireshark network traffic capture window is visible. The filter is set to "ip.dst==182.23.103.155". The capture shows four ICMP Echo (ping) requests from source IP 192.168.43.145 to destination IP 182.23.103.155. The packets are numbered 5897, 5899, 5901, and 5905, with sequence numbers 9/230, 10/25, 11/28, and 12/30 respectively.

No.	Time	Source	Destination	Protocol	Length	Info
→ 5897	5...	192.168.43.145	182.23.103.155	ICMP	74	Echo (ping) request id=0x0001, seq=9/230...
5899	5...	192.168.43.145	182.23.103.155	ICMP	74	Echo (ping) request id=0x0001, seq=10/25...
5901	5...	192.168.43.145	182.23.103.155	ICMP	74	Echo (ping) request id=0x0001, seq=11/28...
5905	5...	192.168.43.145	182.23.103.155	ICMP	74	Echo (ping) request id=0x0001, seq=12/30...

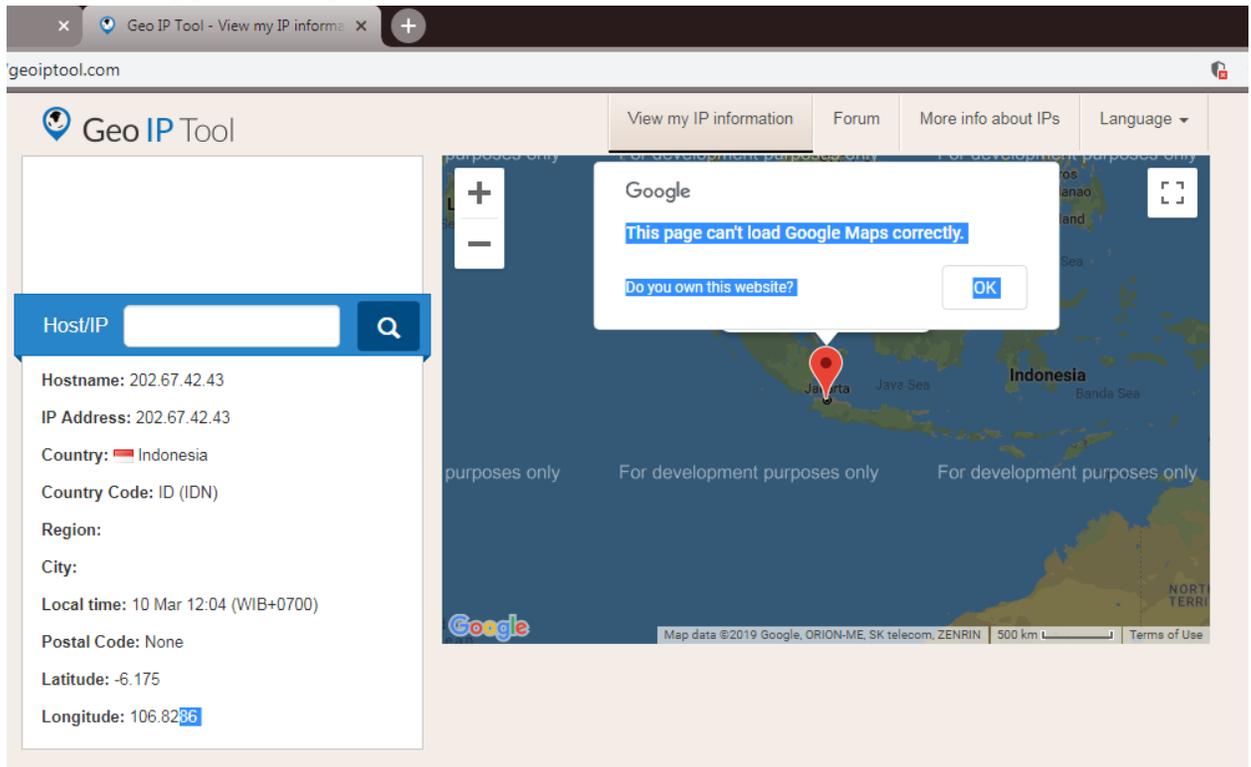
<http://www.cnn.com/> ip address 151.101.65.67

The image shows a screenshot of a web browser displaying the CNN International website. The browser's address bar shows the URL <https://edition.cnn.com>. The website content includes a 'BREXIT WATCH' section with a countdown timer 'Brexit happens in 19d 11h 26m'. The main headline is 'No survivors in Boeing 737 MAX 8 crash', with a sub-headline: 'BREAKING: The Ethiopian Airlines flight is the same model as the Indonesian Lion Air jet that crashed and killed 189 people'. Other news items include 'UK PM braced for possible biggest policy climbdown yet', 'Putin cracks down on freedoms', and '12 dead after plane crashes in Colombia'. A sidebar on the right lists 'In focus' items such as 'Could the US lose this secretive island military base?' and 'Trudeau's 'Lav-Scam' scandal is snowballing'.

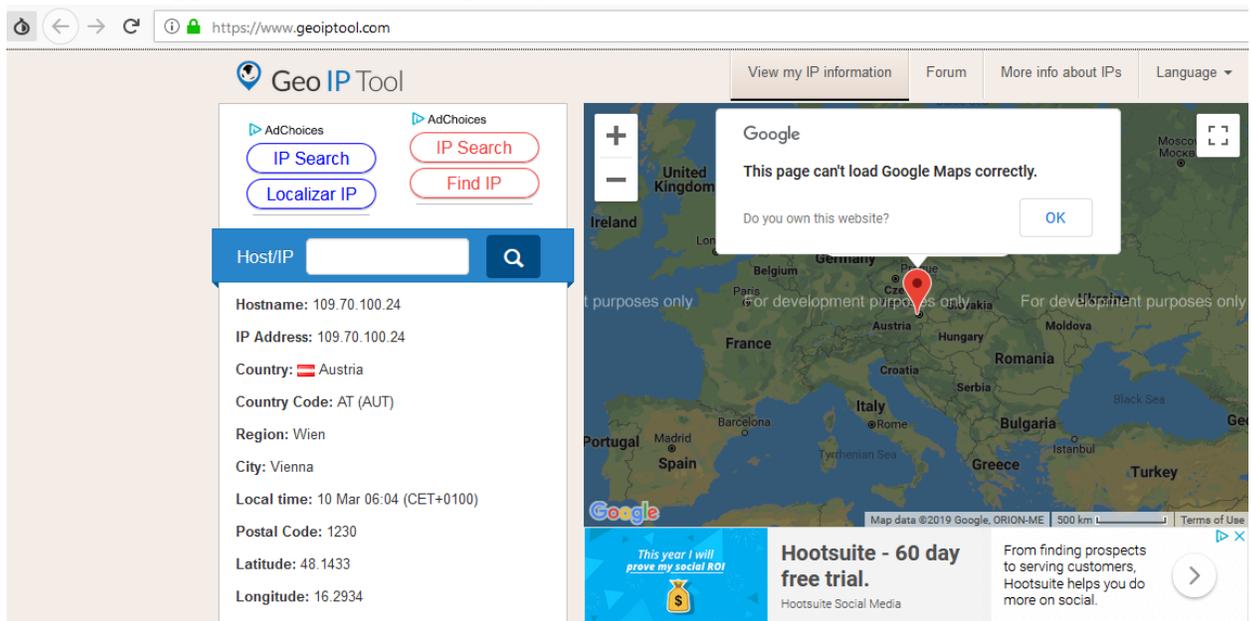
Below the browser window, a network traffic capture window titled '\*Wireless Network Connection' is visible. The filter is set to 'ip.dst==151.101.65.67'. The capture shows four ICMP Echo (ping) requests from source IP 192.168.43.145 to destination IP 151.101.65.67. The packets are numbered 6438, 6444, 6446, and 6453, with sequence numbers 13/33, 14/35, 15/38, and 16/40 respectively.

No.	Time	Source	Destination	Protocol	Length	Info
→ 6438	1...	192.168.43.145	151.101.65.67	ICMP	74	Echo (ping) request id=0x0001, seq=13/33...
6444	1...	192.168.43.145	151.101.65.67	ICMP	74	Echo (ping) request id=0x0001, seq=14/35...
6446	1...	192.168.43.145	151.101.65.67	ICMP	74	Echo (ping) request id=0x0001, seq=15/38...
6453	1...	192.168.43.145	151.101.65.67	ICMP	74	Echo (ping) request id=0x0001, seq=16/40...

- Menggunakan google



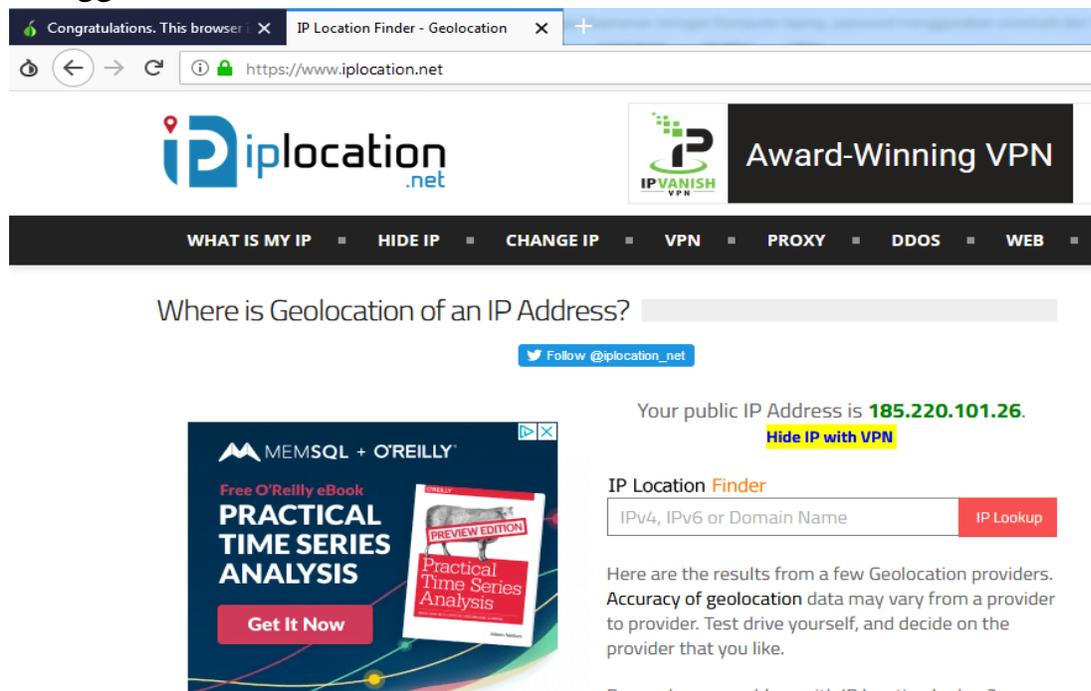
- Menggunakan TOR dengan ip lain



- Tanpa menggunakan TOR browser



- Menggunakan TOR browser



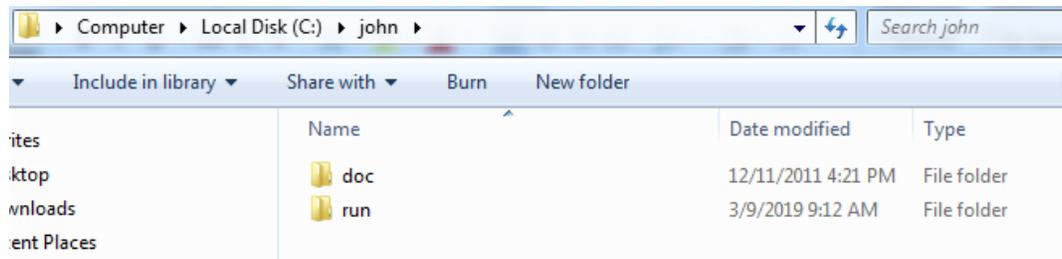
Bisa kita lihat perbedaan server local dari ip lain saat menggunakan TOR browser dan beda ip nya dengan menggunakan google

### 3. Menggunakan John The Ripper

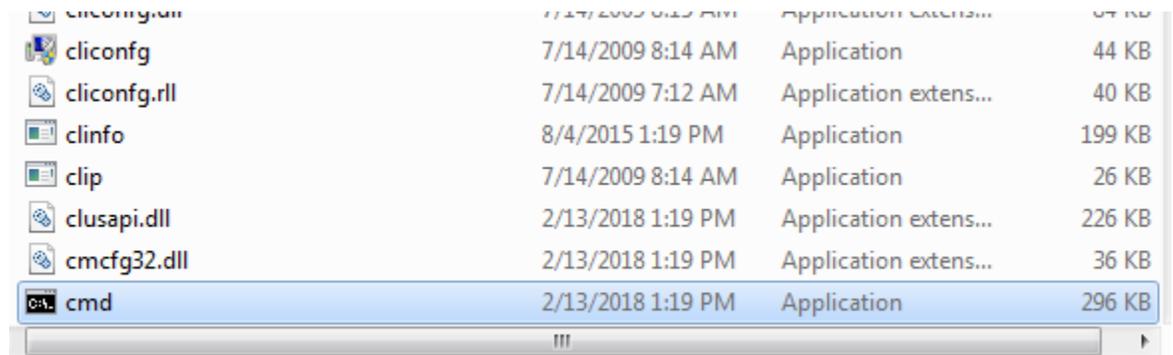
- Pertama kita download aplikasi john the ripper



- Kemudian ekstrak dan buka aplikasi tersebut



- setelah dibuka pilih **run**, dan copy kan cmd(command prompt) kedalam folder cmd.



- didalam folder **RUN**, buka cmd yang sudah dicopy tadi, akan muncul tampilan seperti gambar dibawah ini.



- kemudian kita jalankan dengan cara seperti digambar dibawah ini.

```
C:\john\run>cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\john\run>cd /
C:\>cd john
C:\john>cd run
C:\john\run>john
John the Ripper password cracker, version 1.7.9
Copyright (c) 1996-2011 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single                "single crack" mode
--wordlist=FILE --stdin wordlist mode, read words from FILE or stdin
--rules                enable word mangling rules for wordlist mode
--incremental[=MODE]  "incremental" mode (using section MODE)
--external=MODE       external mode or word filter
--stdout[=LENGTH]    just output candidate passwords [cut at LENGTH]
--restore[=NAME]     restore an interrupted session [called NAME]
--session=NAME       give a new session the NAME
--status[=NAME]     print status of a session [called NAME]
--make-charset=FILE  make a charset, FILE will be overwritten
--show              show cracked passwords
--test[=TIME]       run tests and benchmarks for TIME seconds each
--users=[-]LOGIN:UID[,...] [do not] load this <these> user(s) only
--groups=[-]GID[,...] load users [not] of this <these> group(s) only
--shells=[-]SHELL[,...] load users with[out] this <these> shell(s) only
--salts=[-]COUNT  load salts with[out] at least COUNT passwords only
--save-memory=LEVEL enable memory saving, at LEVEL 1..3
--format=NAME       force hash type NAME: des/bsdi/md5/bf/afs/lm/trip/
                    dummy

C:\john\run>
```