

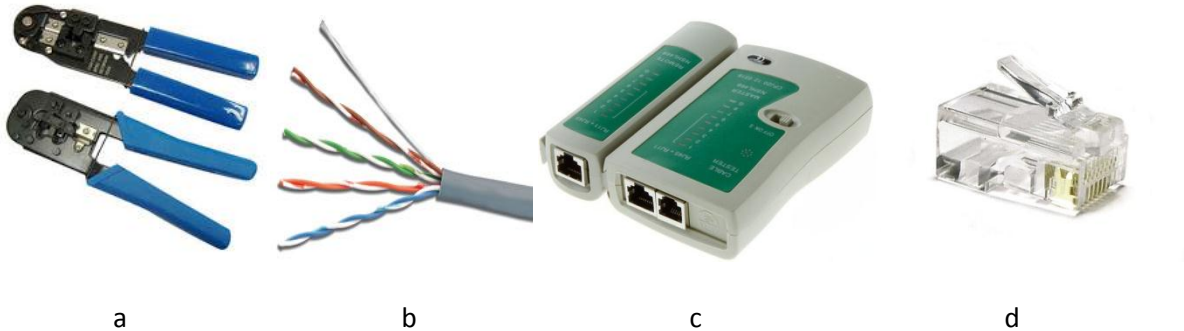
## MODUL 1

### PRAKTIKUM JARINGAN KOMPUTER 2015-2016

#### ANALISIS PAKET DAN PENGKABELAN

## 1. Pengkabelan

### 1.1. Peralatan yang perlu dipersiapkan



Keterangan :

a = Tang crimping

b = kabel STP

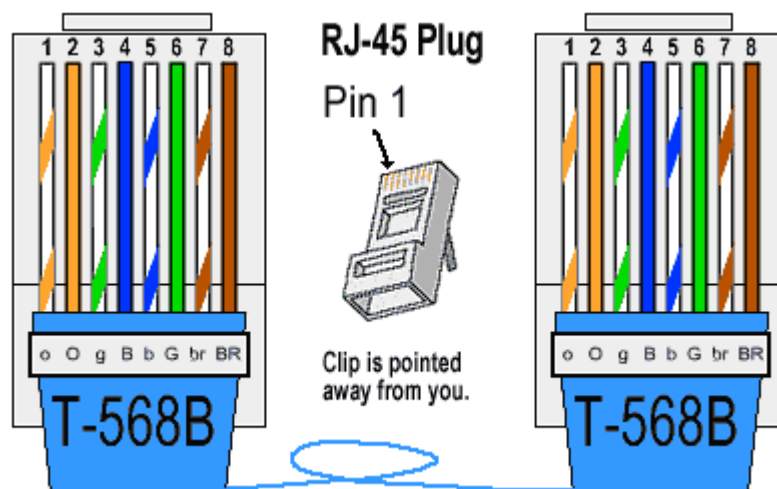
c = Lan tester

d = RJ 45

### 1.2. Jenis Pengkabelan

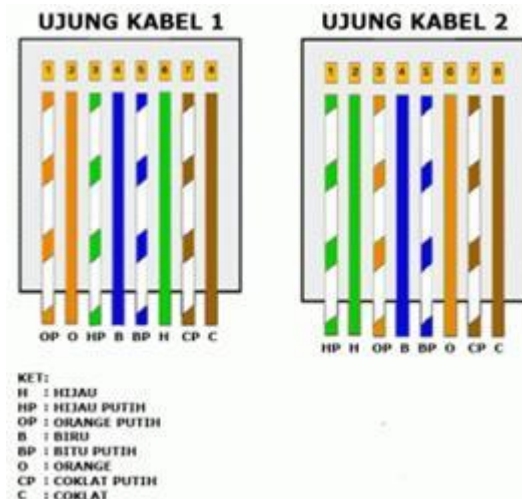
#### 1.2.1. Kabel straight

Kabel straight merupakan kabel yang memiliki cara pemasangan yang sama antara ujung satu dengan ujung yang lainnya. Kabel straight digunakan untuk menghubungkan 2 device yang berbeda, misalnya antara switch dengan router dan komputer dengan switch. Urutan standar kabel straight adalah seperti dibawah ini:



### 1.2.2. Kabel Cross

Kabel cross over merupakan kabel yang memiliki susunan berbeda antara ujung satu dengan ujung dua. Kabel cross over digunakan untuk menghubungkan 2 *device* yang sama. Gambar dibawah adalah susunan standar kabel cross over.



Dari 8 buah kabel yang ada pada kabel UTP ini (baik pada kabel *straight* maupun *cross*) hanya 4 buah saja yang digunakan untuk mengirim dan menerima data, yaitu kabel pada pin no 1,2,3 dan 6.

### 1.3. Cara Crimping

1. Mengupas kulit kabel selebar 2 cm menggunakan tang crimping.
2. Menyusun rapi delapan kabel yang terdapat didalam kabel STP sesuai dengan jenis kabel mana yang ingin dibuat (*straight* atau *cross*).
3. Meluruskan kabel yang masih kusut.
4. Meratakan ujung kabel dengan memotong nya menggunakan tang crimping.
5. memasukan kabel kedalam konektor RJ-45, pastikan ujung kabel menyentuh ujung RJ-45, dan jepitlah menggunakan tang crimping.
6. Lakukan hal serupa pada kedua ujung kabel.
7. Menguji menggunakan LAN tester, jika semua lampu menyala, berarti kabel tersebut telah di crimping dengan benar dan bisa digunakan.

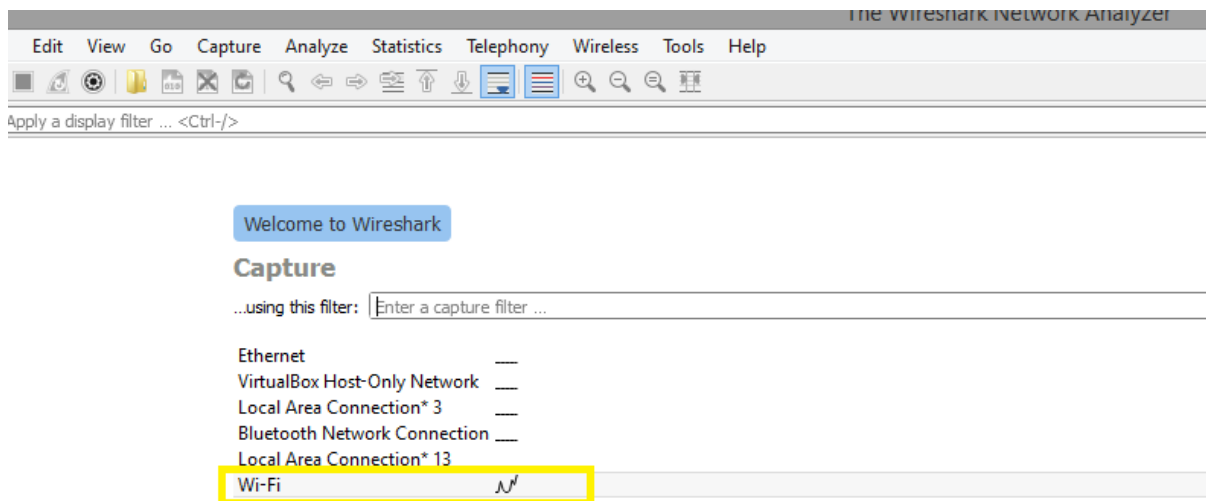
## 2. Analisis Paket dengan Wireshark

### 2.1. Penjelasan dan Instalasi

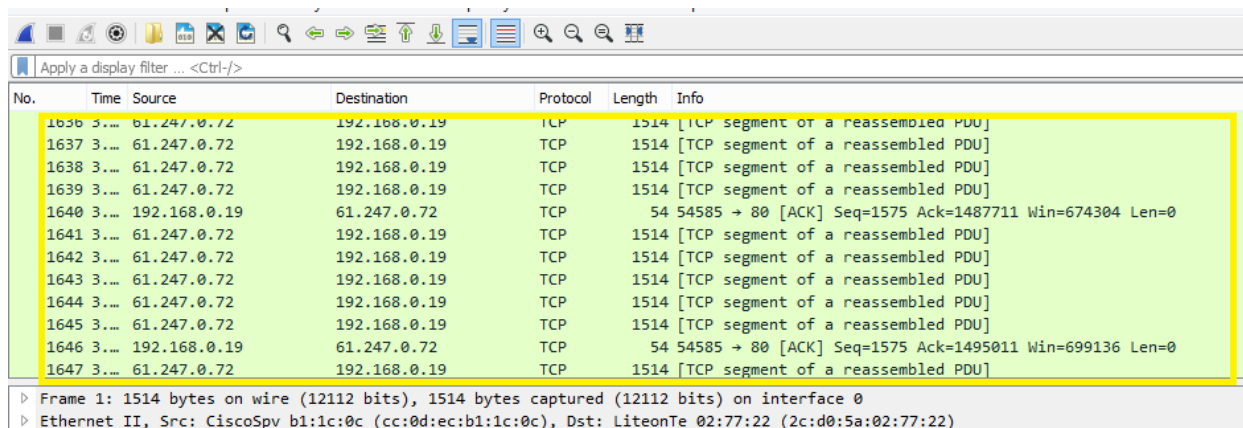
Wireshark adalah aplikasi *sniffing* paket yang dikirim atau diterima perangkat kita. *Sniffing* adalah mencari tahu atau menginspeksi apa isi paket tersebut. Wireshark dapat digunakan untuk *troubleshooting* masalah jaringan. Wireshark dapat didapatkan dari alamat <https://www.wireshark.org/download.html> boleh menggunakan windows ataupun linux. Untuk tutorial instalasi dapat menggunakan dokumen dari wireshark yang berada di laman situs wireshark yang tersedia.

## 2.2. Cara Penggunaan

1. Jalankan Wireshark sebagai *Administrator*. agar dapat menangkap paket yang sedang berjalan.
2. Koneksikan laptop atau komputer yang sedang digunakan dengan Wi-Fi atau LAN.
3. Untuk mempermudah *filter*, Wireshark menyediakan fitur *Capture Filter* sehingga setiap paket yang diterima/dikirim dapat di filter secara otomatis ketika melakukan *Capture Packet*. Untuk menangkap semua paket, kosongkan *capture filter*.
4. Pilih interface yang ingin dipantau oleh Wireshark (Wi-Fi / LAN).



5. Paket yang diterima/terkirim akan otomatis tertangkap dan ditampilkan setelah memilih interface.



6. Untuk mempermudah menganalisa paket yang spesifik (misal dari IP, protokol atau halaman web tertentu), Wireshark menyediakan fitur *Filter Packet*. Caranya dengan menuliskan nama protokol dan sintaks filtering lainnya pada kolom filter. Berikut adalah contoh penggunaan filter untuk melihat paket yang dikirim/diterima melalui protokol TCP.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
tcp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000	61.247.0.72	192.168.0.19	TCP	1514	80 → 54584 [ACK] Seq=1 Ack=1 Win=1181 Len=1460
2	0.000	61.247.0.72	192.168.0.19	TCP	1514	80 → 54584 [ACK] Seq=1461 Ack=1 Win=1181 Len=1460
3	0.000	192.168.0.19	61.247.0.72	TCP	54	54584 → 80 [ACK] Seq=1 Ack=2921 Win=2537 Len=0
4	0.000	61.247.0.72	192.168.0.19	TCP	1514	80 → 54584 [ACK] Seq=2921 Ack=1 Win=1181 Len=1460
5	0.000	61.247.0.72	192.168.0.19	TCP	1514	80 → 54584 [ACK] Seq=4381 Ack=1 Win=1181 Len=1460
6	0.000	192.168.0.19	61.247.0.72	TCP	54	54584 → 80 [ACK] Seq=1 Ack=5841 Win=2537 Len=0
7	0.000	61.247.0.72	192.168.0.19	TCP	1514	80 → 54584 [ACK] Seq=5841 Ack=1 Win=1181 Len=1460
8	0.000	61.247.0.72	192.168.0.19	TCP	1514	80 → 54584 [ACK] Seq=7301 Ack=1 Win=1181 Len=1460
9	0.000	192.168.0.19	61.247.0.72	TCP	54	54584 → 80 [ACK] Seq=1 Ack=8761 Win=2537 Len=0
10	0.000	61.247.0.72	192.168.0.19	TCP	1514	80 → 54584 [ACK] Seq=8761 Ack=1 Win=1181 Len=1460
11	0.000	61.247.0.72	192.168.0.19	TCP	1514	80 → 54584 [ACK] Seq=10221 Ack=1 Win=1181 Len=1460
12	0.000	192.168.0.19	61.247.0.72	TCP	54	54584 → 80 [ACK] Seq=1 Ack=11681 Win=2532 Len=0

▶ Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0  
 ▶ Ethernet II, Src: CiscoSpv\_b1:1c:0c (cc:0d:ec:b1:1c:0c), Dst: LiteonTe\_02:77:22 (2c:d0:5a:02:77:22)  
 ▶ Internet Protocol Version 4, Src: 61.247.0.72, Dst: 192.168.0.19  
 ▶ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 54584 (54584), Seq: 1, Ack: 1, Len: 1460

7. Setelah melakukan filter, pilih paket yang ingin dianalisis. Wireshark secara otomatis akan menampilkan detail paket yang dipilih beserta informasi yang dapat diambil. Berikut contoh detail paket TCP :

▶ Frame 330: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
▶ Ethernet II, Src: CiscoSpv_9c:e6:e2 (34:bd:fa:9c:e6:e2), Dst: IntelCor_a4:d0:60 (00:26:c7:a4:d0:60)
▶ Internet Protocol Version 4, Src: 202.46.129.93, Dst: 192.168.0.111
▲ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 53824 (53824), Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 53824
[Stream index: 15]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
Header Length: 28 bytes
▶ Flags: 0x012 (SYN, ACK)
Window size value: 14600
[Calculated window size: 14600]
▶ Checksum: 0xe226 [validation disabled]
Urgent pointer: 0
▶ Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
▲ [SEQ/ACK analysis]
[This is an ACK to the segment in frame: 329]
[The RTT to ACK the segment was: 0.067282000 seconds]
[iRTT: 0.067397000 seconds]

8. Dari gambar diatas, dapat diambil beberapa informasi misalnya :

- Source IP
- Destination IP
- Source Port
- Destination Port
- Sequence Number
- ACK Number
- Flags (SYN, ACK)

## 2.3. Penggunaan Filter-Filter di Wireshark

### 2.3.1. Capture Filter

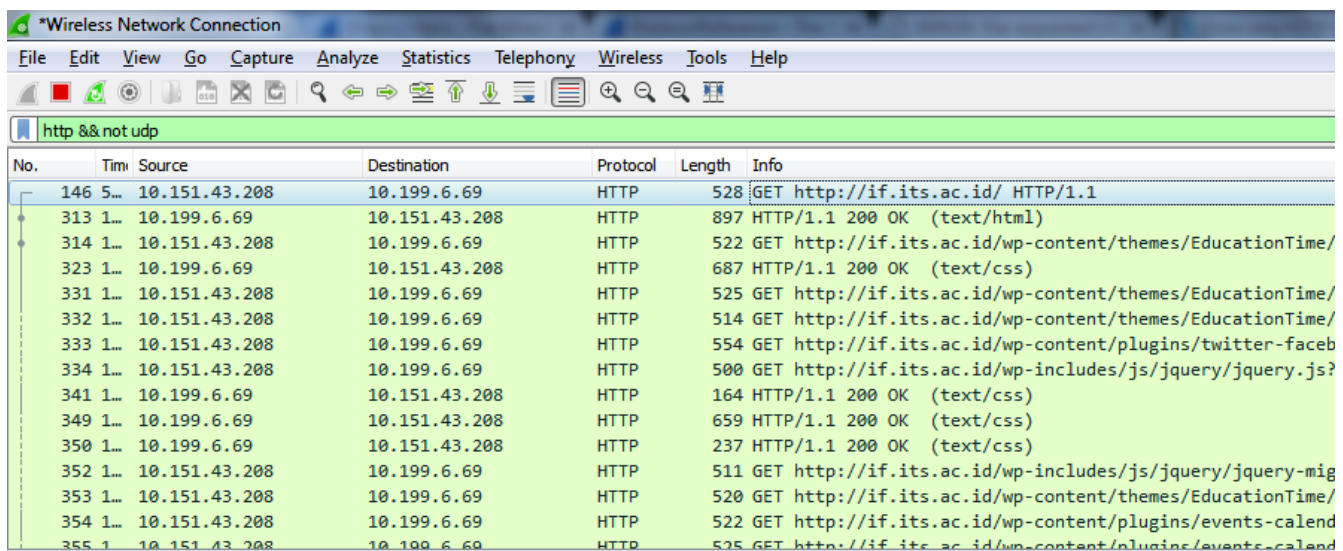
Contoh	Deskripsi
host 192.168.0.1	Hanya menangkap trafik dari atau menuju IP 192.168.0.1
net 192.168.0.0/24 atau net 192.168.0.0 mask 255.255.255.0	Hanya menangkap trafik dari atau menuju range IP 192.168.0.xxx
src net 192.168.0.0/24	Hanya menangkap trafik dari range IP 192.168.0.xxx
port 53	Hanya menangkap trafik dari port 53
Udp	Hanya menangkap trafik menggunakan protokol UDP

### 2.3.2. Display Filter

Contoh	Deskripsi
ip.src == 192.168.0.1    ip.dst == 192.168.0.1	Hanya menampilkan trafik dari atau menuju IP 192.168.0.1
ip.src == 192.168.0.0/24	Hanya menangkap trafik dari range IP 192.168.0.xxx
tcp.port == 25	Hanya menampilkan trafik pada port 25
http.host == "if.its.ac.id"	Hanya menampilkan trafik pada host <i>if.its.ac.id</i>
http.host contains "its.ac.id"	Hanya menampilkan trafik pada host yang namanya mengandung "its.ac.id"

## 2.4. Contoh Penggunaan

### 2.4.1. Basic GET request/reply (website : if.its.ac.id)



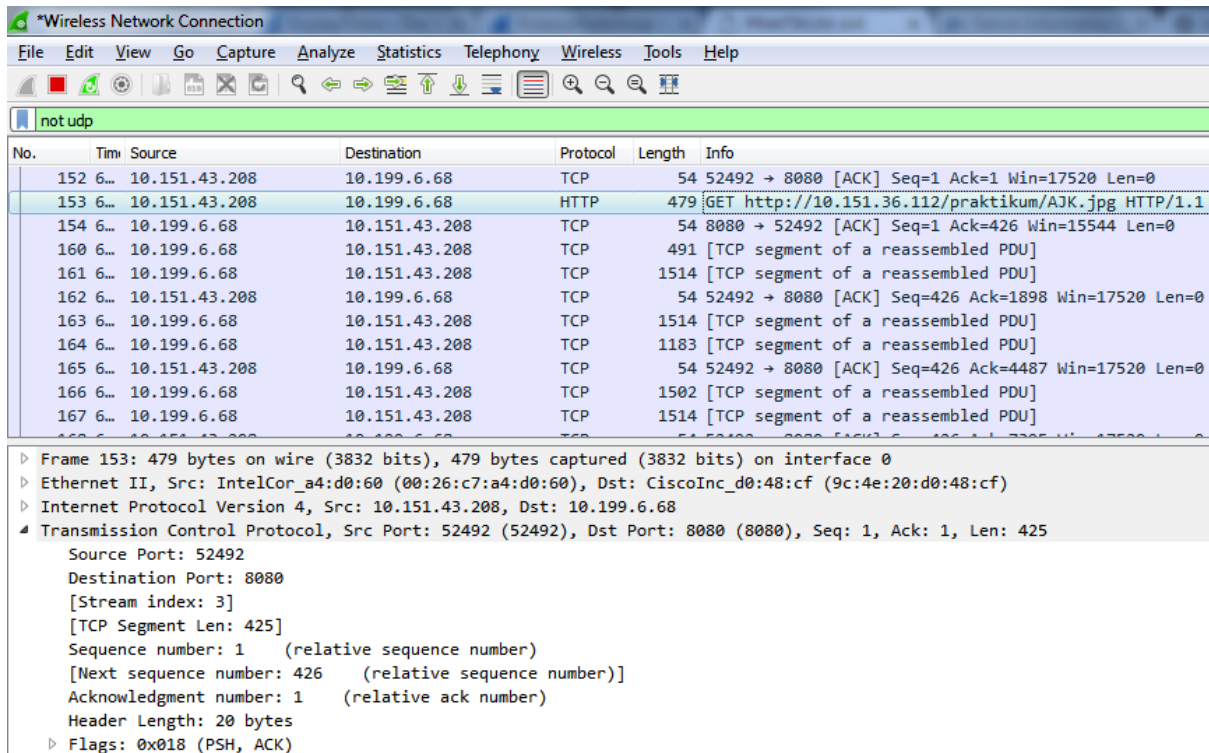
No.	Time	Source	Destination	Protocol	Length	Info
146	5...	10.151.43.208	10.199.6.69	HTTP	528	GET http://if.its.ac.id/ HTTP/1.1
313	1...	10.199.6.69	10.151.43.208	HTTP	897	HTTP/1.1 200 OK (text/html)
314	1...	10.151.43.208	10.199.6.69	HTTP	522	GET http://if.its.ac.id/wp-content/themes/EducationTime/
323	1...	10.199.6.69	10.151.43.208	HTTP	687	HTTP/1.1 200 OK (text/css)
331	1...	10.151.43.208	10.199.6.69	HTTP	525	GET http://if.its.ac.id/wp-content/themes/EducationTime/
332	1...	10.151.43.208	10.199.6.69	HTTP	514	GET http://if.its.ac.id/wp-content/themes/EducationTime/
333	1...	10.151.43.208	10.199.6.69	HTTP	554	GET http://if.its.ac.id/wp-content/plugins/twitter-faceb
334	1...	10.151.43.208	10.199.6.69	HTTP	500	GET http://if.its.ac.id/wp-includes/js/jquery/jquery.js?
341	1...	10.199.6.69	10.151.43.208	HTTP	164	HTTP/1.1 200 OK (text/css)
349	1...	10.199.6.69	10.151.43.208	HTTP	659	HTTP/1.1 200 OK (text/css)
350	1...	10.199.6.69	10.151.43.208	HTTP	237	HTTP/1.1 200 OK (text/css)
352	1...	10.151.43.208	10.199.6.69	HTTP	511	GET http://if.its.ac.id/wp-includes/js/jquery/jquery-mig
353	1...	10.151.43.208	10.199.6.69	HTTP	520	GET http://if.its.ac.id/wp-content/themes/EducationTime/
354	1...	10.151.43.208	10.199.6.69	HTTP	522	GET http://if.its.ac.id/wp-content/plugins/events-calend
355	1...	10.151.43.208	10.199.6.69	HTTP	525	GET http://if.its.ac.id/wp-content/plugins/events-calend

Lakukan juga untuk host website monta.if.its.ac.id dan rbtc.if.its.ac.id

### 2.4.2. Download File dari Web Server

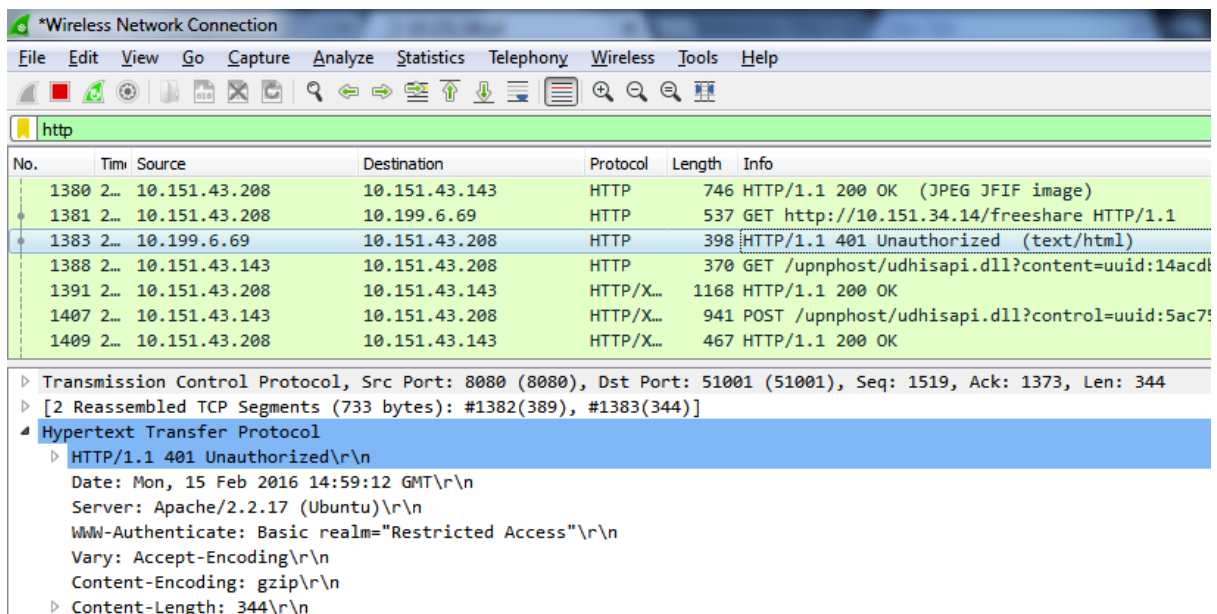
1. Buka halaman <http://10.151.36.112/praktikum/>
2. Masukkan username "praktikum" dan password "praktikumjuga".
3. Buka Wireshark, lalu *start capturing packets*.
4. Klik link download pada halaman <http://10.151.36.112/praktikum/profile.php>.

5. Lalu buka lagi Wireshark dan cari *request* yang dikirim untuk download file. Berikut hasilnya :



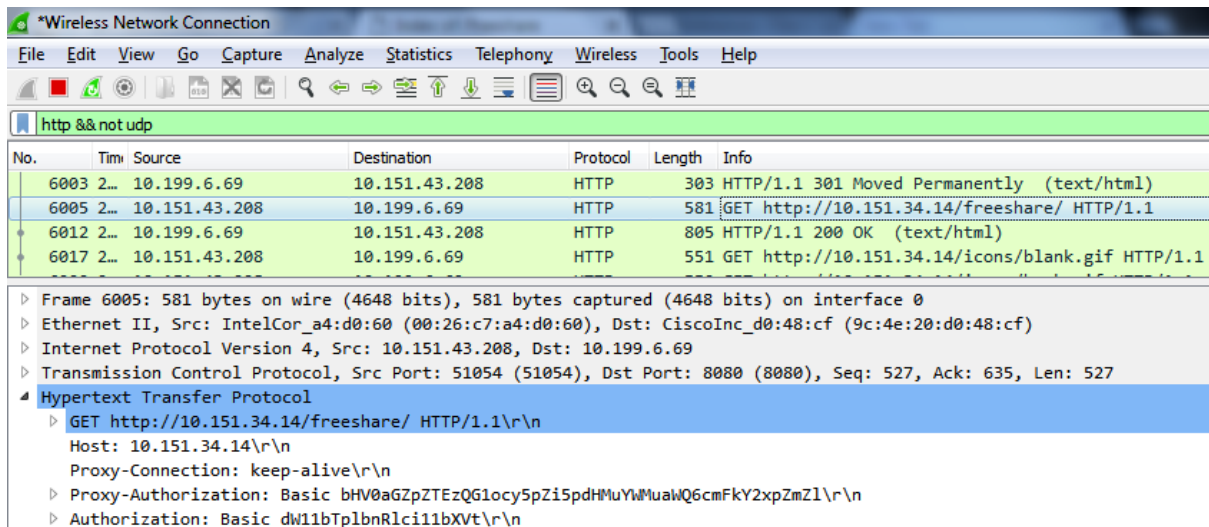
#### 2.4.3. HTTP Basic & Digest Authentication

Sebelum autentikasi (Basic Authentication)

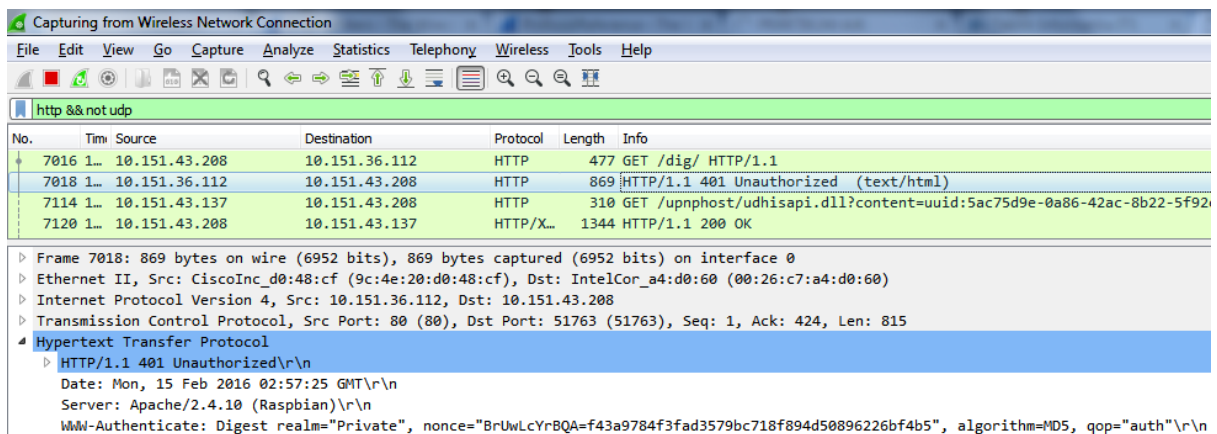




## Setelah autentikasi (Basic Authentication)



## Sebelum autentikasi (Digest Authentication)



### 2.4.4. Non HTTPS authentication

1. Buka halaman <http://10.151.36.112/praktikum/> .
2. Masukkan username "praktikum" dan password "mypassword".
3. Buka Wireshark untuk melihat paket yang terkirim.

Capturing from Wireless Network Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http &&not udp

No.	Time	Source	Destination	Protocol	Length	Info
95	3...	10.151.43.208	10.151.36.112	HTTP	698	POST /praktikum/ HTTP/1.1 (application/x-www-form-urlencoded)
97	3...	10.151.36.112	10.151.43.208	HTTP	780	HTTP/1.1 200 OK (text/html)
249	6...	10.151.43.134	10.151.43.208	HTTP	324	GET /upnphost/udhisapi.dll?content=uuid:5ac75d9e-0a86-42ac-8b22
263	6...	10.151.43.208	10.151.43.134	HTTP/X...	1392	HTTP/1.1 200 OK

Transmission Control Protocol, Src Port: 52024 (52024), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 644

Hypertext Transfer Protocol

POST /praktikum/ HTTP/1.1\r\n

Host: 10.151.36.112\r\n

Connection: keep-alive\r\n

Content-Length: 53\r\n

Cache-Control: max-age=0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n

Origin: http://10.151.36.112\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.109 Safari/537.36\r\n

Content-Type: application/x-www-form-urlencoded\r\n

Referer: http://10.151.36.112/praktikum/\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.8,id;q=0.6\r\n

Cookie: PHPSESSID=1qskbbfp2p6mn1ceojdfnm0vg6\r\n\r\n

[Full request URI: http://10.151.36.112/praktikum/]

[HTTP request 1/1]

[Response in frame: 97]

HTML Form URL Encoded: application/x-www-form-urlencoded

Form item: "username" = "praktikum"

Form item: "password" = "mypassword"

Form item: "submit" = " Login "

## 2.4.5. Akses Website HTTPS

\*Wireless Network Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
3964	1...	10.199.6.69	10.151.43.208	TLSv1.2	539	Application Data
3965	1...	10.199.6.69	10.151.43.208	TLSv1.2	163	Application Data
3967	1...	10.199.6.69	10.151.43.208	TLSv1.2	535	Application Data
3969	1...	10.199.6.69	10.151.43.208	TLSv1.2	203	Application Data
3970	1...	10.151.43.137	239.255.255.250	SSDP	139	M-SEARCH * HTTP/1.1
3987	1...	10.151.43.208	10.199.6.69	HTTP	346	CONNECT www.facebook.com:443 HTTP/1.1
3989	1...	10.199.6.69	10.151.43.208	HTTP	93	HTTP/1.1 200 Connection established
3990	1...	10.151.43.208	10.199.6.69	TLSv1.2	571	Client Hello
3997	1...	10.151.43.137	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
4002	1...	10.199.6.69	10.151.43.208	TLSv1.2	200	Server Hello, Change Cipher Spec, Encrypted Handshake Message
4003	1...	10.151.43.208	10.199.6.69	TLSv1.2	105	Change Cipher Spec, Hello Request, Hello Request
4004	1...	10.151.43.208	10.199.6.69	TLSv1.2	107	Application Data
4005	1...	10.151.43.208	10.199.6.69	TLSv1.2	104	Application Data
4006	1...	10.151.43.208	10.199.6.69	TLSv1.2	96	Application Data
4008	1...	10.151.43.208	10.199.6.69	TLSv1.2	910	Application Data

Frame 3987: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) on interface 0

Ethernet II, Src: IntelCor\_a4:d0:60 (00:26:c7:a4:d0:60), Dst: CiscoInc\_d0:48:cf (9c:4e:20:d0:48:cf)

Internet Protocol Version 4, Src: 10.151.43.208, Dst: 10.199.6.69

Transmission Control Protocol, Src Port: 50734 (50734), Dst Port: 8080 (8080), Seq: 1, Ack: 1, Len: 292

Hypertext Transfer Protocol

CONNECT www.facebook.com:443 HTTP/1.1\r\n

Host: www.facebook.com:443\r\n

Proxy-Connection: keep-alive\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.109 Safari/537.36\r\n

Proxy-Authorization: Basic bHV0aGZpZTEzQG1ocy5pZi5pdHMuYmMuahQ6cmFkY2xpZmZl\r\n\r\n

[Full request URI: http://www.facebook.com:443www.facebook.com:443]

[HTTP request 1/1]

[Response in frame: 3989]



## 2.4.6. Akses Website Melalui Proxy ITS

The image shows a Wireshark packet capture titled "Wireless Network Connection". The filter is set to "http && not udp". The packet list shows four packets:

No.	Time	Source	Destination	Protocol	Length	Info
3909	9...	10.151.43.208	10.199.6.69	HTTP	528	GET http://if.its.ac.id/ HTTP/1.1
3978	9...	10.151.43.137	10.151.43.208	HTTP	310	GET /upnphost/udhisapi.dll?content=uuid:5ac75d9e-0a86--
3984	9...	10.151.43.208	10.151.43.137	HTTP/X...	1344	HTTP/1.1 200 OK
4062	9...	10.199.6.69	10.151.43.208	HTTP	897	HTTP/1.1 200 OK (text/html)

The packet details for packet 3909 are expanded, showing:

- Frame 3909: 528 bytes on wire (4224 bits), 528 bytes captured (4224 bits) on interface 0
- Ethernet II, Src: IntelCor\_a4:d0:60 (00:26:c7:a4:d0:60), Dst: CiscoInc\_d0:48:cf (9c:4e:20:d0:48:cf)
- Internet Protocol Version 4, Src: 10.151.43.208, Dst: 10.199.6.69
- Transmission Control Protocol, Src Port: 50876 (50876), Dst Port: 8080 (8080), Seq: 398, Ack: 3904, Len: 474
- Hypertext Transfer Protocol
  - GET http://if.its.ac.id/ HTTP/1.1\r\n
  - Host: if.its.ac.id\r\n
  - Proxy-Connection: keep-alive\r\n
  - Proxy-Authorization: Basic bHV0aGZpZTEzQG1ocy5pZi5pdHMuYmMuawQ6cmFkY2xpZmZl\r\n
  - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n
  - Upgrade-Insecure-Requests: 1\r\n
  - User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.109 Safari/537.36\r\n
  - Accept-Encoding: gzip, deflate, sdch\r\n
  - Accept-Language: en-US,en;q=0.8,id;q=0.6\r\n

## 2.4.7. FTP

Buka FileZilla, lalu masukkan data berikut :

Host : 10.151.36.112

Username : pi

Password : raspberry

The image shows the FileZilla interface. The Host is set to 10.151.36.112, Username is pi, and Password is masked. The Status bar shows the connection process: Connecting to 10.151.36.112:21..., Connection established, waiting for welcome message..., Insecure server, it does not support FTP over TLS., Connected, Retrieving directory listing..., and Directory listing of "/" successful.

The Local site is E:\ (Master) and the Remote site is /. The Remote site directory listing is shown below:

Filename	Filesize	Filetype	Last modified	Permissions
..				
.cache		File folder	02/02/2016 22:...	flcdmpe (0...
.config		File folder	02/02/2016 22:...	flcdmpe (0...
.dbus		File folder	02/02/2016 22:...	flcdmpe (0...
.gstream...		File folder	02/02/2016 22:...	flcdmpe (0...
.local		File folder	15/02/2016 10:...	flcdmpe (0...
.node-gyp		File folder	02/02/2016 22:...	flcdmpe (0...

Mengakses server ftp dengan filezilla.

*Wireless Network Connection						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
not udp && ftp						
No.	Time	Source	Destination	Protocol	Length	Info
193...	6...	10.151.36.112	10.151.43.208	FTP	119	Response: 220 ProFTPD 1.3.5 Server (10.151.36.112) [::ffff:10.151.36.112]
193...	6...	10.151.43.208	10.151.36.112	FTP	64	Request: AUTH TLS
193...	6...	10.151.36.112	10.151.43.208	FTP	79	Response: 500 AUTH not understood
193...	6...	10.151.43.208	10.151.36.112	FTP	64	Request: AUTH SSL
193...	6...	10.151.36.112	10.151.43.208	FTP	79	Response: 500 AUTH not understood
193...	6...	10.151.43.208	10.151.36.112	FTP	63	Request: USER pi
193...	6...	10.151.36.112	10.151.43.208	FTP	84	Response: 331 Password required for pi
193...	6...	10.151.43.208	10.151.36.112	FTP	70	Request: PASS raspberry
193...	6...	10.151.36.112	10.151.43.208	FTP	77	Response: 230 User pi logged in
193...	6...	10.151.43.208	10.151.36.112	FTP	60	Request: SYST
193...	6...	10.151.36.112	10.151.43.208	FTP	73	Response: 215 UNIX Type: L8
Frame 19342: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface 0						
Ethernet II, Src: CiscoInc_d0:48:cf (9c:4e:20:d0:48:cf), Dst: IntelCor_a4:d0:60 (00:26:c7:a4:d0:60)						
Internet Protocol Version 4, Src: 10.151.36.112, Dst: 10.151.43.208						
Transmission Control Protocol, Src Port: 21 (21), Dst Port: 52733 (52733), Seq: 1, Ack: 1, Len: 65						
Source Port: 21						
Destination Port: 52733						
[Stream index: 299]						
[TCP Segment Len: 65]						
Sequence number: 1 (relative sequence number)						
[Next sequence number: 66 (relative sequence number)]						
Acknowledgment number: 1 (relative ack number)						
Header Length: 20 bytes						
Flags: 0x018 (PSH, ACK)						
Window size value: 29200						
[Calculated window size: 29200]						
[Window size scaling factor: -2 (no window scaling used)]						
Checksum: 0x8ac7 [validation disabled]						

Keluaran sniffing di wireshark

### 3. Latihan

1. Ketika mengakses suatu halaman web, berapakah port yang dituju oleh suatu paket?
2. Apa sajakah perbedaan ketika mengakses halaman utama website `if.its.ac.id`, `monta.if.its.ac.id`, dan `rbtc.if.its.ac.id`? Jelaskan jawaban anda.
3. Ada berapa jumlah paket yang dikirimkan oleh web server ketika mengunduh file? Mengapa terjadi yang seperti itu?
4. Dari hasil analisa paket, apa perbedaan ketika menggunakan persistent connection dan non-persistent connection?
5. Apa perbedaan ketika autentikasi menggunakan method basic dengan digest?
6. Apa perbedaan ketika mengakses halaman web biasa dengan ketika proses login terjadi?
7. Apa saja yang selalu dikirimkan browser ke web server?
8. Apa perbedaan ketika mengakses suatu website dengan dan tanpa proxy?
9. Perintah apa saja yang dikirimkan oleh FTP client ketika login?
10. Perintah apa saja yang dikirimkan oleh FTP client ketika melihat isi direktori, upload, dan download?
11. Perintah apa saja yang dikirimkan oleh FTP client ketika menyalin, memindahkan, dan menghapus file?

**Referensi :**

<https://aslibumiayu.wordpress.com/2011/01/21/cara-buat-krimping-kabel-jaringan/>

<http://www.adalahcara.com/2013/06/cara-crimping-kabel-utp-ke-rg-45.html>

<https://www.wireshark.org/>

<http://wiki.wireshark.org/DisplayFilters>

<http://wiki.wireshark.org/CaptureFilters>