PRAKTIKUM 5: WIRESHARK

Pertemuan ke : 5

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Skor Penilaian : 100 %
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK

CPL-6	Memahami tanggung jawab profesional dan menerapkan pengetahuan serta berkomunikasi efektif dalam melakukan penilaian berdasar informasi dan praktek computing dengan berpedoman pada prinsip-prinsip legal dan etika
CPMK-03	Mahasiswa mampu menganalisa digital evidence dan pengolahan bukti digital

5.1. TUJUAN DAN INDIKATOR CAPAIAN

Setelah mengikuti praktikum ini mahasiswa diharapkan;
1. Praktikan mampu menganalisis digital evidence berupa artefact network
2. Praktikan mampu melakukan filtering parameter network

5.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-06	CPMK-03	Kemampuan mahasiswa menganalisis berupa bookmark evidence dan merepresentasikan hasil temuan

5.3. TEORI PENDUKUNG

Wireshark adalah program Network Protocol Analyzer alias penganalisa protokol jaringan yang lengkap. Program ini dapat merakam semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin, misalnya postingan komentar kamu di blog atau bahkan Username dan Password.

Secara garis besar cara kerja wireshark terdiri dari dua tahapan yaitu:

1. Merekam semua paket yang melewati interface yang dipilih (Interface adalah perangkat penghubung antar jaringan, bisa melalui wifi atau ethernet / lan card)
2. Hasil rekaman tadi dapat dianalisa. disini kita dapat memfilter protocol apa yang kita inginkan seperti tcp, http, udp dan sebagainya. Wireshark juga dapat mencatat cookie, post dan request. Filtering dalam wireshark:
   - Http : Hanya paket http yang akan ditampilkan
   - Ip.addr ==x.x.x.x : Hanya akan menampilakn ip address yang dimaksud, (ganti xxxx menjadi ip address)
   - Ip.addr ==x.x.x.x && ip.addr == x.x.x.x : menampilkan ip address dengan logika and, artinya paket yang ditampilkan hanya jika kondisinya ada dua ip address tersebut dalam paket.
   - http.request : Menampilkan paket http dengan status post atau get.
   - Tcp contains xxx : Menampiknan paket TCP yang mengandung kata XXX

- !(aro or icmp or dns) : Dibaca not arp or icmp or dns. Artinya paket arp atau icmp atau dns tidak akan ditampikan .
- http.request.uri contains “xxx” : perintah untuk mencari kata/kalimat apa yang di ketik/search
- xml.cdata contains “preview-url” : untuk memfilter preview-url yang telah dibuka

5.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Aplikasi Wireshark.

5.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-03	Apa yang dimaksud dengan pacet capture network kaitannya dalam live forensics?	50
2.	CPL-06	CPMK-03	Sebutkan beserta kelebihan tools network analisis selain wireshark!	50

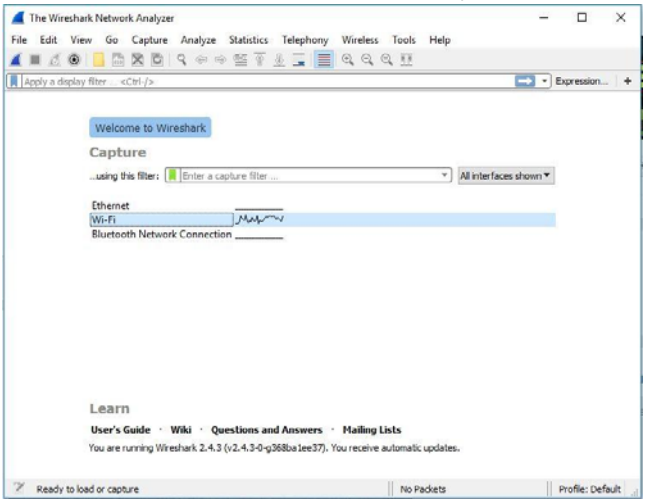
5.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-06	CPMK-03	Selesaikan langkah praktikum berikut!	Screen Shot Hasil praktikum	100

Ikuti langkah dibawah ini:

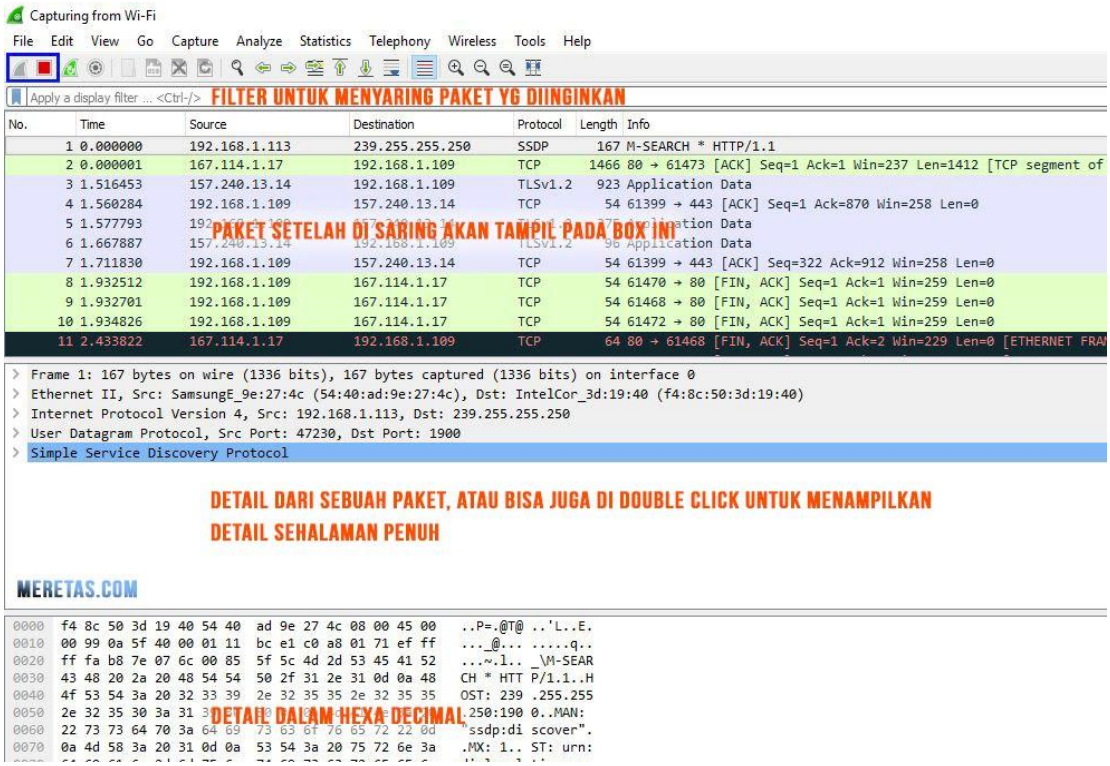
1. Install aplikasi wireshark
2. Setelah menginstal wireshark, akan muncul halaman awal seperti ini



Gambar 5.1 Page Awal Wireshark.

Semua interface akan ditampilkan beserta diagram gelombang yang menadakan bahwa ada paket data yang melewati interface tersebut.

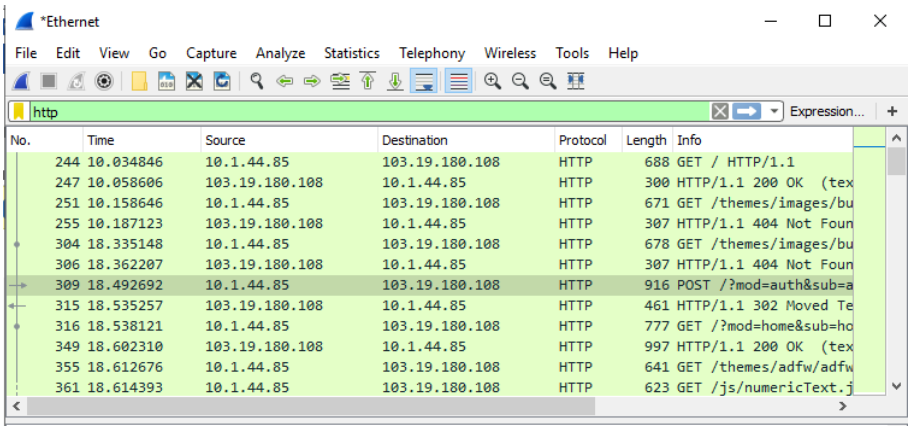
3. Klik dua kali pada interface yang akan digunakan untuk mengcapture paket data. Maka akan muncul tampilan seperti ini



Gambar *5*.2 Wireshark Capture Trafict

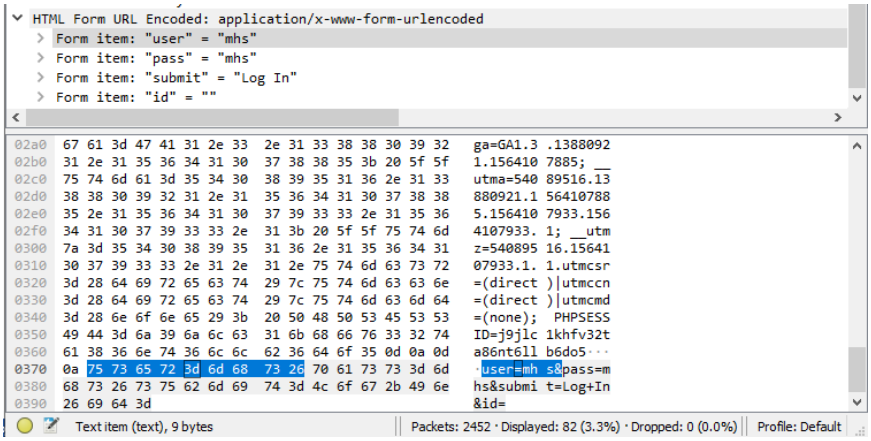
Semua detail paket akan ditampilkan, seperti asal IP address, protokol sebagainya.

4. Coba login ke halaman web yang tidak terenkripsi (http) lalu melakukan filtering paket http. (Pada praktikum ini kita coba pakai simeru.uad.ac.id)



Gambar *5*.3 Wireshark Capture Filtering

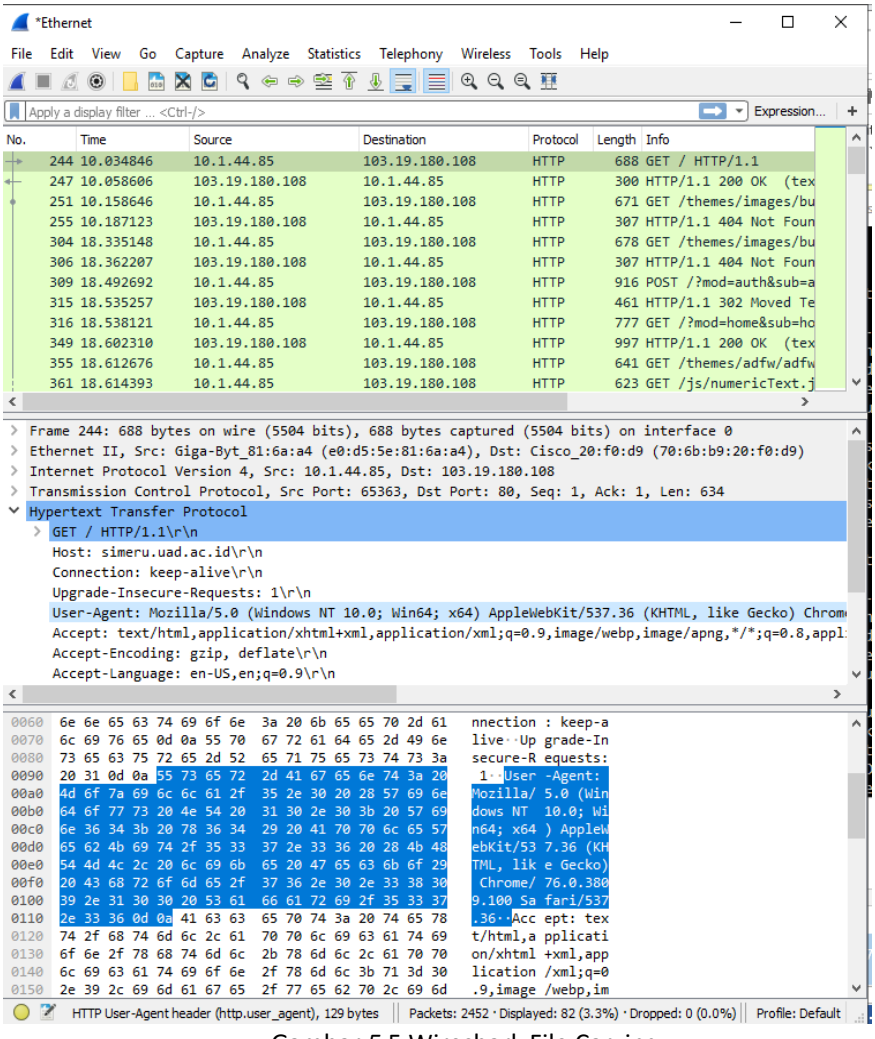
5. Membuka tiap request POST dengan mengklik dua kali paket tersebut satu persatu.



Gambar 5.4 Wireshark Capture Prot Request

Cek setiap Form HTML. Formulir seperti kolom username dan password akan ditemukan di detail HTML Form Url.

6. Untuk mengetahui MAC addess dapat dilakukan dengan cara cek ip asal, lalu klik dua kali, didapat MAC addess dan User-agent yaitu E0:D5:5E:81:6A:A4 Dan user agent Mozila/5.0 (Windows)



Gambar 5.5 Wireshark File Carving

5.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-03	Lakukan proses capture network anda menggunakan tools wireshark, koneksi internet bisa menggunakan tetering dari smartphone anda, kemudian lakukan analisis traffict network anda!	100

5.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-06	CPMK-03	20%		
2.	Praktik	CPL-06	CPMK-03	30%		
3.	Post-Test	CPL-06	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**