PRAKTIKUM 6: SOSIAL CHAT FORENSICS

Pertemuan ke : 6

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-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah
CPMK-02	Mahasiswa mampu merekontruksi skenario kasus menggunakan tools forensik

6.1. TUJUAN DAN INDIKATOR CAPAIAN

Setelah mengikuti praktikum ini mahasiswa diharapkan:
1. Praktikan mampu membuat skenario kasus dari salah satu aplikasi chat
2. Praktikan mampu mengektraksi diigtal evidence instant messenger

6.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-07	CPMK-02	Kemampuan mahasiswa dalam menganalisis sosial chat dan digital evidencenya

6.3. 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.

Macam-macam protokol dan fungsinya di jaringan komputer:

1. TCP/IP (Transmission Control Protocol/Internet Protocol)

   Adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. TCP/IP mengimplemenasikan arsitektur berlapis yang terdiri atas empat lapis, diantaranya adalah :
   a) Protokol lapisan aplikasi
   b) Protokol lapisan antar-host
   c) Protokol lapisan internetwork
   d) Protokol lapisan antarmuka jaringan

2. UDP (User Datagram Protokol)

   UDP, singkatan dari User Datagram Protocol, adalah salah satu protokol lapisan transpor TCP/IP yang mendukung komunikasi yang tidak andal (unreliable), tanpa koneksi (connectionless) antara host-host dalam jaringan yang menggunakan TCP/IP.
   a) Connectionless (tanpa koneksi): Pesan-pesan UDP akan dikirimkan tanpa harus dilakukan proses negosiasi koneksi antara dua host yang hendak berukar informasi.

b) Unreliable (tidak andal): Pesan-pesan UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan acknowledgment. Protokol lapisan aplikasi yang berjalan di atas UDP harus melakukan pemulihan terhadap pesan-pesan yang hilang selama transmisi.
c) UDP menyediakan mekanisme untuk mengirim pesan-pesan ke sebuah protokol lapisan aplikasi atau proses tertentu di dalam sebuah host dalam jaringan yang menggunakan TCP/IP. Header UDP berisi field Source Process Identification dan Destination Process Identification.
d) UDP menyediakan penghitungan checksum berukuran 16-bit terhadap keseluruhan pesan UDP.

3. DNS (Domain Name System)

Domain Name System (DNS) adalah distribute database system yang digunakan untuk pencarian nama komputer (name resolution) di jaringan yang mengunakan TCP/IP (Transmission Control Protocol/Internet Protocol). DNS biasa digunakan pada aplikasi yang terhubung ke Internet seperti web browser atau e-mail, dimana DNS membantu memetakan host name sebuah komputer ke IP address. Selain digunakan di Internet, DNS juga dapat di implementasikan ke private network atau intranet dimana DNS memiliki keunggulan seperti:

a) Mudah, DNS sangat mudah karena user tidak lagi direpotkan untuk mengingat IP address sebuah komputer cukup host name (nama Komputer).
b) Konsisten, IP address sebuah komputer bisa berubah tapi host name tidak berubah.
c) Simple, user hanya menggunakan satu nama domain untuk mencari baik di Internet maupun di Intranet.

4. HTTP (Hypertext Transfer Protocol)

HTTP (Hypertext Transfer Protocol) suatu protokol yang digunakan oleh WWW (World Wide Web). HTTP mendefinisikan bagaimana suatu pesan bisa diformat dan dikirimkan dari server ke client. HTTP juga mengatur aksi-aksi apa saja yang harus dilakukan oleh web server dan juga web browser sebagai respon atas perintah-perintah yang ada pada protokol HTTP ini.

Contohnya bila kita mengetikkan suatu alamat atau URL pada internet browser maka web browser akan mengirimkan perintah HTTP ke web server. Web server kemudian akan menerima perintah ini dan melakukan aktivitas sesuai dengan perintah yang diminta oleh web browser. Hasil aktivitas tadi akan dikirimkan kembali ke web browser untuk ditampilkan kepada kita.

5. HTTPS

https adalah versi aman dari HTTP, protokol komunikasi dari World Wide Web. Ditemukan oleh Netscape Communications Corporation untuk menyediakan autentikasi dan komunikasi tersandi dan penggunaan dalam komersi elektris. Selain menggunakan komunikasi plain text, HTTPS menyandikan data sesi menggunakan protokol SSL (Secure Socket layer) atau protokol TLS (Transport Layer Security). Kedua protokol tersebut memberikan perlindungan yang memadai dari serangan eavesdroppers, dan man in the middle attacks. Pada umumnya port HTTPS adalah 443.

Tingkat keamanan tergantung pada ketepatan dalam mengimplementasikan pada browser web dan perangkat lunak server dan didukung oleh algorithma penyandian yang aktual. Oleh karena itu, pada halaman web digunakan HTTPS, dan URL yang digunakan dimulai dengan ‘https://’ bukan dengan ‘http://’

6. FTP (File Transfer Protocol)

FTP (File Transfer Protocol) adalah sebuah protocol internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pentransferan berkas (file) computer antar mesin-mesin dalam sebuah internetwork.

7. SSL (Secure Socket Layer)

SSL (Secure Socket Layer) adalah arguably internet yang paling banyak digunakan untuk enkripsi. Ditambah lagi, SSL digunakan tidak hanya keamanan koneksi web, tetapi untuk berbagai aplikasi yang memerlukan enkripsi jaringan end-to-end.

Secure Sockets Layer (SSL) merupakan sistem yang digunakan untuk mengenkripsi pengiriman informasi pada internet, sehingga data dapat dikirim dengan aman. Protokol SSL mengatur keamanan dan integritas menggunakan enkripsi, autentikasi, dan kode autentikasi pesan.

6.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Wireshark

6.5. PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-02	Jelaskan apa yang dimaksud dengan Live Forensics Investigation!	50
2.	CPL-07	CPMK-02	Apa kelebihan wireshark dibanding tools forensik lain ?	50

6.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-02	Selesaikan langkah praktikum berikut ini!	Screenshot Hasil praktikum	100

Pada praktikum kali ini menggunakan kasus dari Ann Dercover yang bekerja pada perusahaan yang bernama Anaechy-R-Us, Inc. Namun, perusahaan menaruh curiga kepada Ann. Ann memiliki akses ke resep rahasia perusahaan. Staff keamanan mencurigai Ann kalau kalau si Ann membocorkan rahasia perusahaan. Staff keamanan memonitor perlakuan Ann, tapi tidak ada hal mencurigakan sampai saat ini. Hingga tiba – tiba ada sebuah laptop yang muncul di jaringan perusahaan, dan IP Ann (**192.168.1.158**) mengirim IMs ke laptop tersebut. Laptop tersebut tiba – tiba menghilang sesaat setelah IMs selesai dikirim. Staff keamanan berhasil mengcapture paket yang dikirim dari komputer Ann, dan mereka meminta penulis untuk menganalisis paket tersebut.

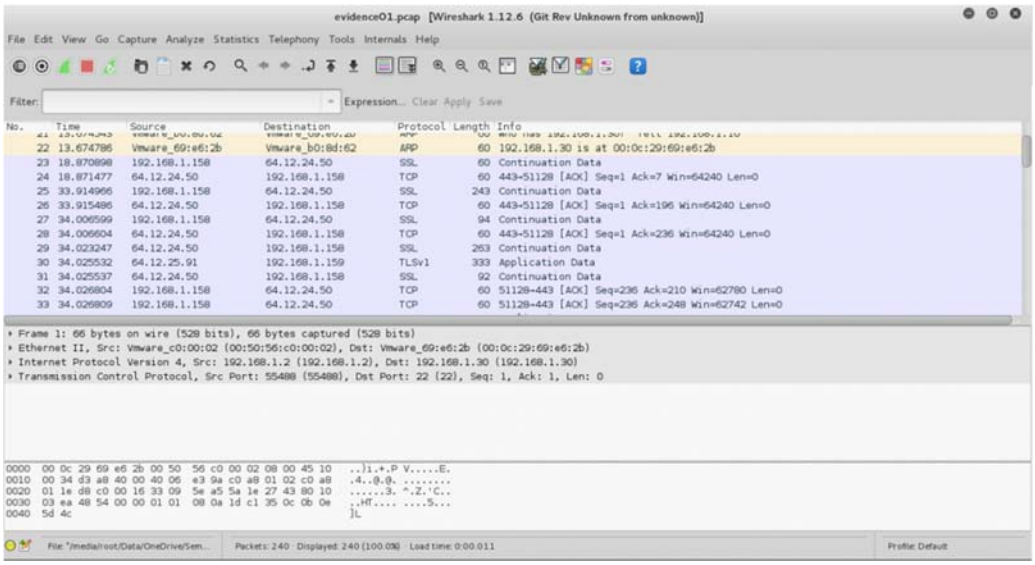
Pertanyaan:

1. Apa nama dari teman IM Ann?
2. Apa komentar pertama dalam percakapan IM ditangkap?
3. Apa nama file Ann yang ditransfer?

Ikuti langkah berikut:

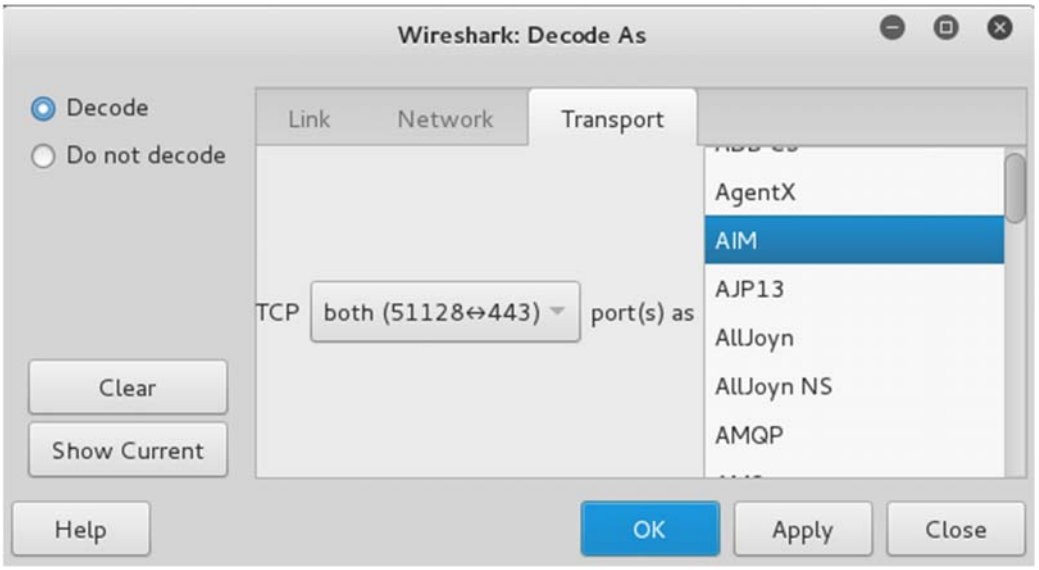
Download capture wireshark pada Link tersedia

Menjawab pertanyaan pertama, maka hal pertama yang harus dilakukan adalah melihat jenis paket apa saja yang ada di wireshark. Ketika kita scroll, akan terlihat tampilan berikut Pada kolom Protocol, ada protokol ARP, TCP, dan SSL.



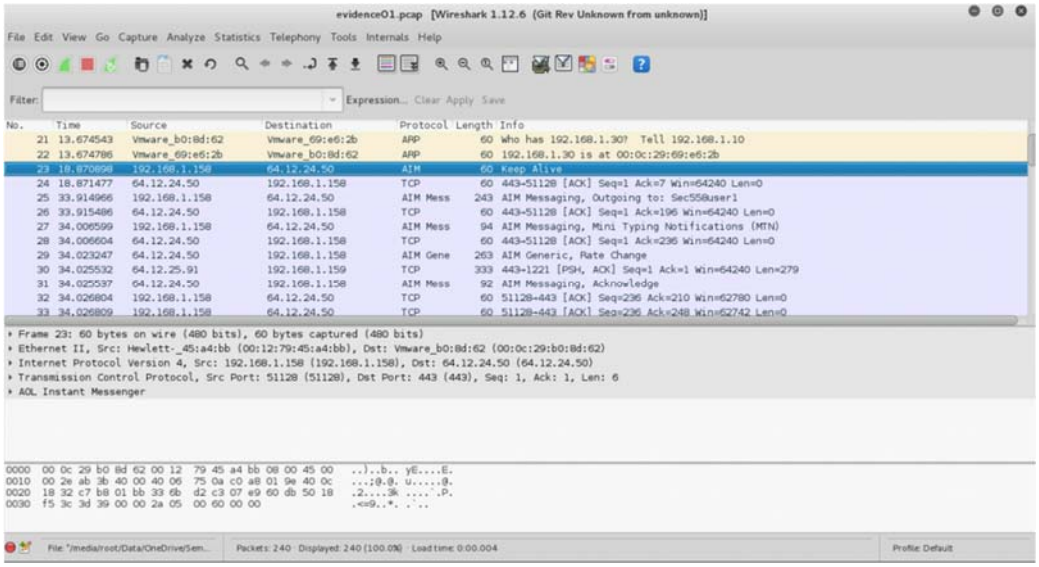
Gambar *6*.1 Pacet Capture Evidence.

Dari analisis staff keamanan, diketahui bahwa protokol yang dipakai adalah AIM yang bekerja di port 443. Secara default, wireshark akan menganggap port 443 adalah port SSL.
Ganti SSL di wireshark menjadi protokol AIM dengan cara **klik kanan paket SSL Decode As AIM**



Gambar *6*.2 Evidence Decode

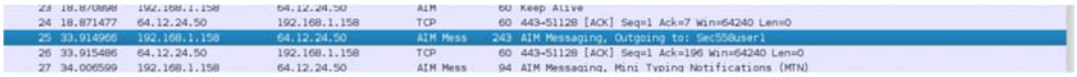
Setelah diklik Apply, maka tampilan wireshark akan menjadi seperti berikut



Gambar *6*.3 Pacet Capture File Carving

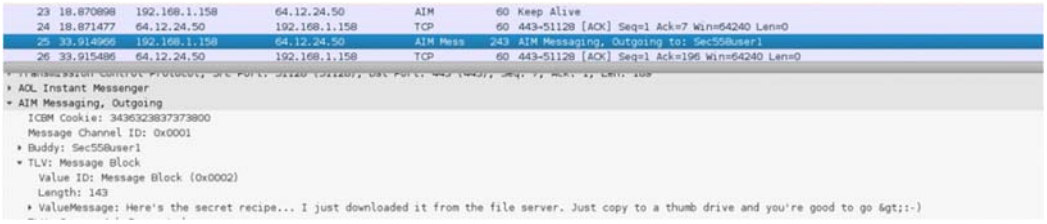
Terlihat pada kolom protokol, SSL telah berubah menjadi AIM. Tujuan perubahan ini agar paket AIM dapat terbaca.

Pada paket nomor 25 terlihat ada kata Outgoing to: Sec558user1.



Maka **Sec558user1** adalah user AIM dari Ann, terjawab pertanyaan nomor 1.

Menjawab pertanyaan ke 2, pada paket yang sama, kita dapat melihat text message yang ada pada paket tersebut.

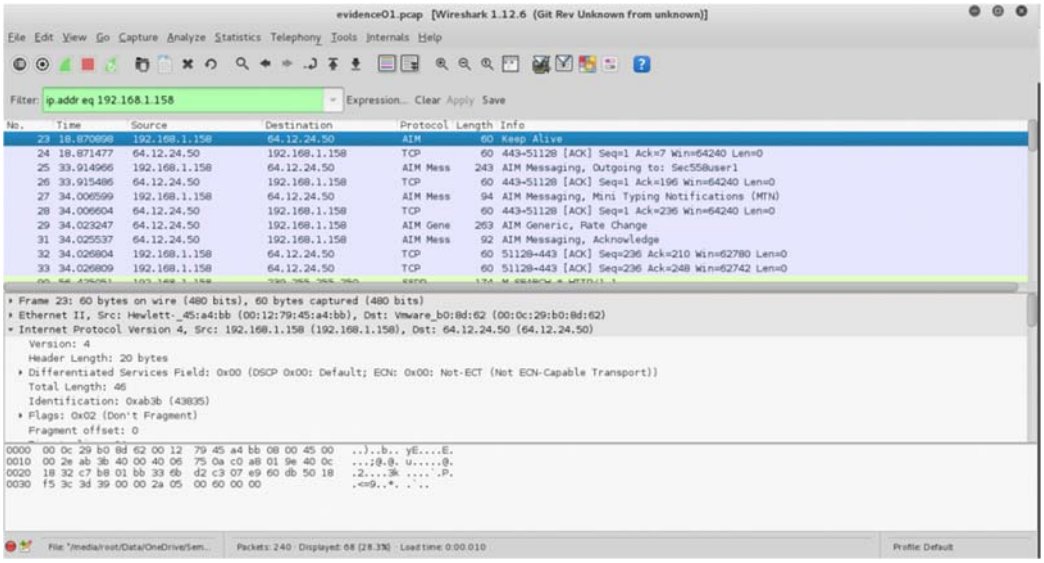


Gambar *6*.4 Pacet Capture Information Carving

Ada kalimat **Here's the secret recipe....**

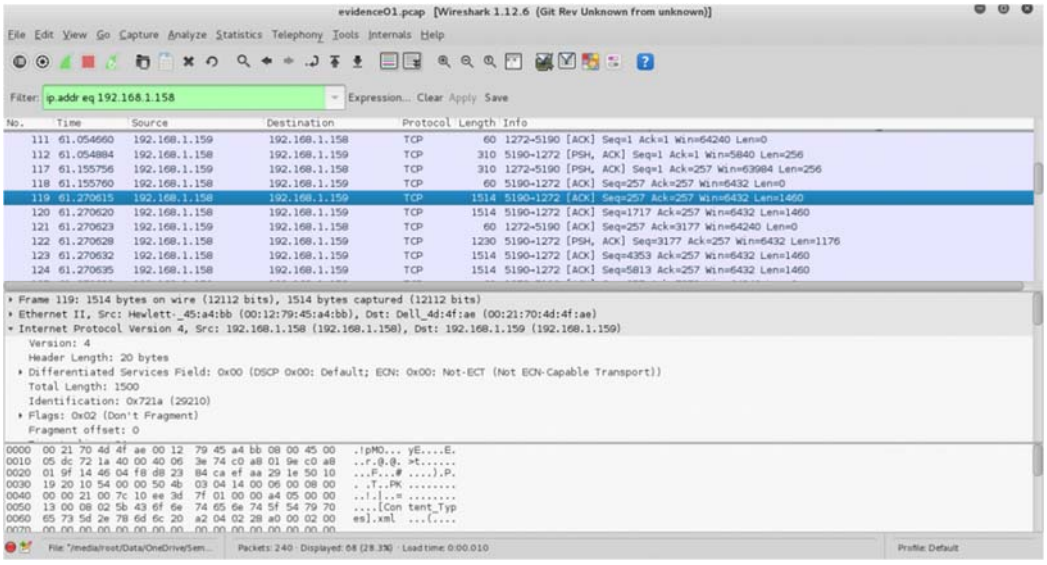
Kalimat tersebut adalah kalimat yang dikirim Ann ke pelaku.

Untuk menjawab nomor 3, kita gunakan filter ip.addr eq 192.168.1.158 , agar dapat menemukan paket yang berasal dari IP 192.168.1.158.



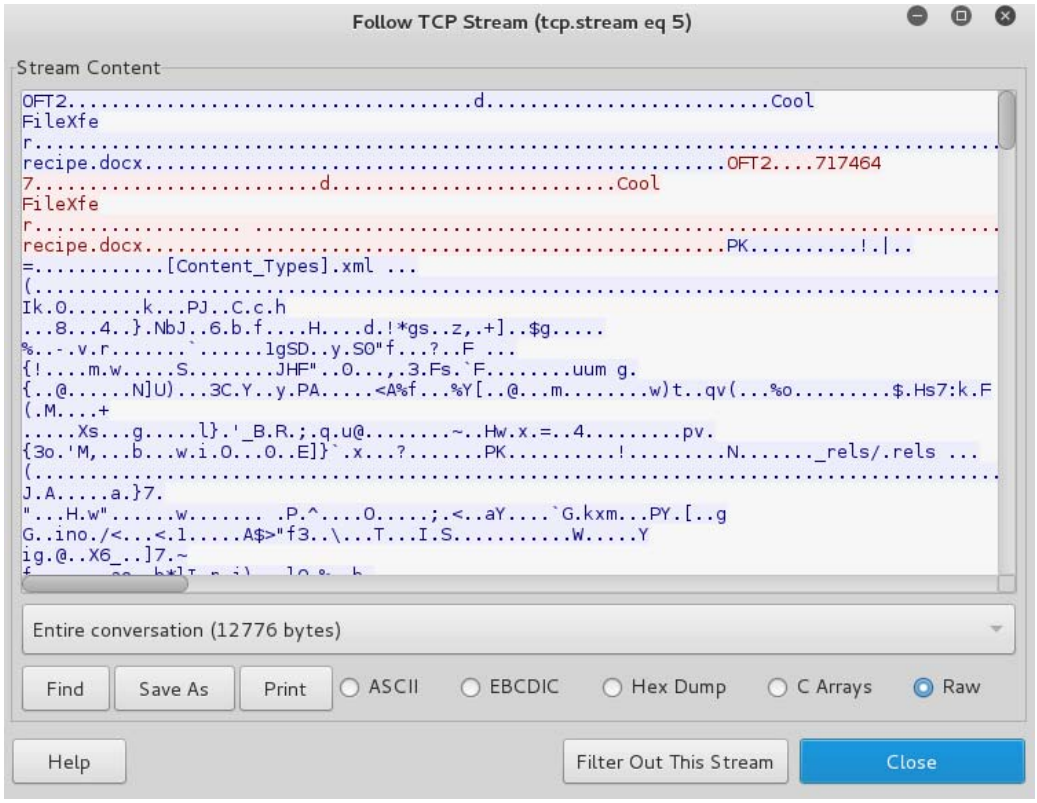
Gambar *6*.5 Pacet Capture information

Setelah mendapatkan filter tersebut, lalu cari yang kolom **length** nya cukup besar. Hal ini dikarenakan yang kita cari adalah paket yang mengirim file.
Dari hasil filter ditemukan pada paket 119 dengan panjang paket 1514, seperti gambar berikut



Gambar *6*.6 Pacet Capture Filtering

Klik kanan pada file tersebut, klik Follow TCP Stream, hasilnya sebagai berikut



Gambar *6*.7 Pacet Capture information Translate Text Find

Maka kita ketahui file yang dikirim adalah file **recipe.docx**

6.7. POST TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-02	1. Apa nama dari teman IM Ann? 2. Apa komentar pertama dalam percakapan IM ditangkap? 3. Apa nama file Ann yang ditransfer?	100

Tugas berisi post test yang harus dikerjakan oleh mahasiswa sebagai evaluasi dari praktikum yang dilakukan (contoh lembar evaluasi terlampir).

6.8. 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-07	CPMK-02	20%		
2.	Praktik	CPL-07	CPMK-02	30%		
3.	Post-Test	CPL-07	CPMK-02	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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