SUMMARY KULIAH UMUM DIGITAL FORENSIK

BARANG BUKTI DATA LIVE STREAMING

Muhamad Adillah Fatih

121103017

A. Introduction

Dalam kuliah umum mengenai digital forensik, pembukaan membahas pentingnya informasi dan konsep-konsep dasar yang terkait dengan pengamanan informasi. Pertama, informasi ditekankan sebagai aset yang sangat berharga dan tersebar di berbagai tempat dengan akses yang luas. Informasi tidak lagi terbatas pada dokumen fisik atau perangkat komputer saja, tetapi dapat ditemukan di perangkat mobile, media sosial, cloud storage, dan berbagai platform online.

Kemudian, pembukaan juga menyoroti kerugian yang dapat terjadi jika informasi tidak dijaga dengan baik. Informasi yang tidak terlindungi bisa disalahgunakan oleh pihak yang tidak bertanggung jawab, seperti pelaku kejahatan cyber atau peretas. Kehilangan data sensitif, pencurian identitas, atau kerugian finansial dapat terjadi sebagai akibat dari kebocoran informasi yang tidak dijaga dengan baik.

Selanjutnya, pembukaan kuliah umum mengenai digital forensik memperkenalkan konsep C-I-A Triad (Confidentiality, Integrity, Availability) dalam menjaga informasi. Konsep ini merupakan dasar dalam upaya melindungi informasi. Confidentiality (kerahasiaan) bertujuan untuk memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang. Integrity (integritas) berkaitan dengan keaslian dan keutuhan informasi, yaitu memastikan bahwa informasi tidak dimanipulasi atau dirusak dengan sengaja. Terakhir, Availability (ketersediaan) mengacu pada ketersediaan informasi yang diperlukan oleh pihak yang berwenang saat dibutuhkan.  
  
Selanjutnya, dalam kuliah umum mengenai digital forensik, akan dibahas tentang ancaman-ancaman terhadap informasi. Terdapat beberapa sumber ancaman yang dapat merusak keamanan dan integritas informasi. Ancaman tersebut bisa karena bad guy, bad code, insider, juga human error. Dalam kuliah umum ini, juga akan dijelaskan beberapa metode yang digunakan oleh penyerang untuk mencapai tujuan mereka. Metode penyerangan seperti phising, password cracking, dan melalui malware.

B. Digital Forensics

Digital forensik adalah proses mengumpulkan, menganalisis, menyediakan bukti elektronik untuk tujuan investigasi. Tujuannya adalah untuk sebagai bukti/jejak digital yang digunakan dalam persidangan. Selain itu untuk improvisasi sistem keamanan.

Siapa yang dapat melakukan kegiatan ini(digital forensik)? Sebetulnya semua orang dapat melakukan ini, namun biasanya yang melakukan forensik digital untuk kebutuhan tertentu adalah cybersecurity agencies, law enforcement agencies, corporate cybersecurity team, dan professionals.

Langkah-langkah untuk melakukan digital forensik berbeda-beda, untuk standarnya adalah identification, preservation, acquisition, analysis, interpretation, hingga documentation & reporting.

C. Live Forensics

Respons langsung mengacu pada proses pengumpulan dan analisis bukti digital dari sistem yang sedang berjalan atau langsung. Lakukan live forensics investigation pada critical system yang tidak boleh mati, juga lakukan analisis malware, serta lakukan investigasi pada saat serangan sedang terjadi.

Step by step live forensics, dimulai dengan planning seperti define objective, identify scope, identify tools required. Lalu Preparation seperti menyiapkan tempat kerja forensik, menyiapkan koneksi untuk kerja remote. Lalu Documentation seperti mengabadikan keadaan sistem saat ini(saat belum melakukan investigasi), waktu, IP, user aktif, aplikasi yang dibuka, dll. Selanjutnya Volatile data collection dan terakhir adalah Memory Acquisition.