



**YAYASAN SASMITA JAYA GROUP**  
**UNIVERSITAS PAMULANG**

Fakultas Ilmu Komputer  
Program Studi Sistem Informasi

SK MENDIKNAS NO. 136/D/O/2001

Jl. Puspiptek Raya No 10, Serpong - Tangerang Selatan Telp. (021) 742 7010, 741 2566  
www.unpam.ac.id



---

---

**LEMBAR JAWABAN**  
**UJIAN AKHIR SEMESTER GENAP**  
**TAHUN AKADEMIK 2023 / 2024**

---

Nama	: Arif Frima Ari Suwadi	Mata Kuliah	: Komputer Forensik
NIM	: 221011700443	Nama Dosen	: Endin Fahrudin,.ST,.MKom
Semester / Kelas	: 04 / 04SIFE003		

---

**Jawaban!**

- Forensik digital sangat diperlukan dalam penyelidikan berbagai kasus karena:
  - Prevalensi bukti digital: Di era modern, sebagian besar informasi dan aktivitas tersimpan dalam bentuk digital. Ini mencakup komunikasi, transaksi keuangan, hingga data lokasi.
  - Kompleksitas teknologi: Kejahatan semakin canggih dan sering melibatkan teknologi. Forensik digital membantu mengungkap bukti yang tersembunyi atau dienkripsi.
  - Integritas bukti: Teknik forensik digital memastikan bahwa bukti dikumpulkan, dianalisis, dan disajikan dengan cara yang dapat diterima secara hukum.
  - Rekonstruksi kejadian: Memungkinkan penyidik untuk merekonstruksi urutan peristiwa digital, yang sangat penting dalam memahami kronologi kejadian.
  - Pengungkapan informasi tersembunyi: Dapat mengungkap data yang telah dihapus atau disembunyikan, yang mungkin krusial untuk kasus.
  - Analisis pola: Membantu mengidentifikasi pola perilaku atau aktivitas yang mungkin tidak terlihat tanpa analisis digital mendalam.
  - Efisiensi penyelidikan: Mempercepat proses investigasi dengan kemampuan untuk memproses dan menganalisis sejumlah besar data secara cepat.
- Digital forensik dapat mengungkap berbagai jenis informasi, termasuk:
  - Riwayat aktivitas perangkat: Kapan perangkat digunakan, aplikasi apa yang diakses, dan berapa lama.

- b) File yang dihapus atau tersembunyi: Menggunakan teknik khusus untuk memulihkan data yang telah dihapus atau disembunyikan.
  - c) Metadata file: Informasi tentang file seperti waktu pembuatan, modifikasi, dan akses terakhir.
  - d) Komunikasi digital: Email, pesan teks, panggilan telepon, dan aktivitas media sosial.
  - e) Riwayat internet: Situs yang dikunjungi, pencarian yang dilakukan, dan file yang diunduh.
  - f) Data lokasi: Informasi GPS dari perangkat mobile yang menunjukkan pergerakan pengguna.
  - g) Aktivitas jaringan: Koneksi ke jaringan Wi-Fi atau seluler, log akses server.
  - h) Informasi sistem: Konfigurasi perangkat, aplikasi yang terinstal, dan pembaruan sistem.
  - i) Data cloud: Informasi yang tersimpan di layanan penyimpanan online.
  - j) Jejak keuangan digital: Transaksi online, penggunaan cryptocurrency, atau aktivitas perbankan digital.
  - k) Bukti manipulasi: Indikasi apakah file atau data telah diubah atau dipalsukan.
3. Kebutuhan forensik komputer dalam penyelidikan meliputi:
- a) Perangkat keras khusus:
    - Write blockers untuk mencegah modifikasi data asli
    - Perangkat penyimpanan forensik berkapasitas tinggi
    - Workstation forensik yang kuat untuk analisis data besar
  - b) Perangkat lunak forensik:
    - Tools untuk akuisisi dan analisis data seperti EnCase, FTK, atau Autopsy
    - Software untuk pemulihan data yang dihapus
    - Alat analisis malware dan keamanan jaringan
  - c) Laboratorium forensik:
    - Ruang yang terkontrol untuk mencegah kontaminasi elektromagnetik
    - Sistem keamanan untuk menjaga integritas bukti
    - Peralatan anti-statis untuk menangani komponen sensitif
  - d) Prosedur dan metodologi:
    - Protokol standar untuk pengumpulan dan penanganan bukti digital
    - Metode dokumentasi yang rinci untuk setiap langkah analisis

- 
- 
- Prosedur chain of custody untuk melacak penanganan bukti
- e) Sumber daya manusia:
- Ahli forensik digital yang terlatih dan bersertifikasi
  - Analis keamanan siber untuk kasus yang melibatkan serangan jaringan
  - Ahli hukum yang memahami aspek legal dari bukti digital
- f) Penyimpanan dan pengarsipan:
- Sistem penyimpanan aman dengan enkripsi untuk bukti digital
  - Fasilitas pengarsipan jangka panjang untuk kasus yang berkelanjutan
- g) Pelatihan dan pengembangan:
- Program pelatihan berkelanjutan untuk mengikuti perkembangan teknologi
  - Akses ke sumber daya penelitian dan pengembangan forensik terbaru
- h) Kerjasama dan networking:
- Hubungan dengan lembaga penegak hukum dan forensik lainnya
  - Akses ke database kejahatan dan informasi intelijen
- i) Manajemen kasus:
- Sistem manajemen kasus untuk melacak dan mengelola bukti digital
  - Software untuk pelaporan dan presentasi hasil analisis forensik