Nama:

Npm :

Kelas:

1. Jelaskan tahapan komputer forensik!
2. Pada tahap pengujian, terdapat tahap:

* By passing fitur sistem
* Filtrasi
* Mengexclude file
* Mengalokasi file
* Mengestrak file

Jelaskan!

1. Berikan contoh hal yang dapat digunakan sebagai bukti! (min 5)
2. Apa itu auction fraud – online? Jelaskan & beri contoh!
3. Jelaskan tentang memory Imaging Techniques (2 saja)!

=============================================================

1. **Tahapan komputer forensik:**

a). Pengumpulan Data

Pengumpulan data bertujuan untuk meng­i­den­tifikasi berbagai sumber daya yang dianggap penting dan bagaimana semua data dapat terhimpun dengan­ baik.

b)     Pengujian

Pengujian mencakup proses penilaian dan meng-ekstrak berbagai informasi yang relevan dari semua data yang dikumpulkan. Tahap ini juga mencakup bypassing proses atau meminimalisasi berbagai feature­ sistem operasi dan aplikasi yang dapat menghilangkan data, seperti kompresi, enkripsi, dan akses mekanisme kontrol. Cakupan lainnya adalah meng­alokasi file, mengekstrak file, pemeriksanan meta data, dan lain sebagainya.

c)      Analisis

Analisis dapat dilakukan dengan menggunakan pendekatan sejumlah metode. Untuk memberikan kesimpulan yang berkualitas­ harus didasarkan pada ketersediaan sejumlah data atau bahkan sebaliknya, dengan menyimpulkan bahwa “tidak ada kesimpulan”. Hal tersebut sa­ngat dimungkinan­kan. Tugas analisis ini mencakup­ berbagai kegia­tan, seperti identifikasi user atau orang di luar pengguna yang terlibat secara tidak langsung, lokasi, perangkat, kejadiaan, dan mempertimbangkan bagaimana semua komponen tersebut saling terhubung hingga mendapat kesimpulan akhir.

d)     Dokumentasi dan laporan

Ada beberapa faktor yang mempengaruhi hasil­ dokumentasi dan laporan, seperti:

* Alternative Explanations (Penjelasan Alternatif)

Berbagai penjelasan yang akurat seharusnya dapat menjadi sebuah pertimbangan untuk diteruskan dalam proses reporting. Seorang analis seharusnya mampu menggunakan sebuah pendekatan berupa metode yang menyetujui atau menolak setiap penjelasan sebuah perkara yang diajukan.

* Audience Consideration (Pertimbangan Penilik)

Menghadirkan data atau informasi keseluruh audience sangat berguna. Kasus yang melibatkan sejumlah aturan sangat membutuhkan laporan secara spesifik berkenaan dengan informasi yang dikumpulkan. Selain itu, dibutuhkan­ pula copy dari setiap fakta (evidentiary data) yang diperoleh. Hal ini dapat menjadi sebuah pertimbangan yang sangat ber­alasan. Contohnya, jika seorang Administrator Sistem sebuah jaringan sangat memungkinkan untuk mendapatkan dan melihat­ lebih dalam sebuah network traffic dengan informasi yang lebih detail.

* Actionable Information

Proses dokumentasi dan laporan mencakup pula tentang identifikasi actionable information yang didapat dari kumpulan­ sejumlah data terdahulu. Dengan­ bantuan data-data tersebut, Anda juga bisa mendapatkan dan meng­ambil berbagai informasi terbaru.

1. **Tahapan pengujian:**
2. By passing fitur-fitur sistem

Meminimalisir fitur-fitur sistem operasi dan sistem aplikasi yang akan mengaburkan data, seperti kompresi, enkripsi dan akses mekanisme kontrol.

1. Filtrasi

Mengeliminir sebagian data yang tidak dibutuhkan, misanya data log minggu lalu yang terdiri dari jutaan record dan didapati hanya ratusan record saja yang dinilai penting untuk pemeriksaan lebih lanjut.

1. Mengexclude file

Memasukan file sebagai data yang dibutuhkan.

1. Mengalokasikan file

Menempatkan setiap berkas pada satu himpunan blok yang berurut didalam disk.

1. Mengekstrak file

adalah salah satu perintah di komputer untuk membedah/membuka suatu **file** Arsip seperti berekstensi.

1. **Hal yang dapat digunakan sebagai bukti:**

* Audio recorder
* Mesin penjawab
* Kabel
* Peralatan caller ID
* Telpon selular

1. **Auction Fraud – Online**

Penipuan lelang internet yang melibatkan skema yang dapat dikaitkan dengan salah satu produk yang diiklankan untuk dijualkan melalui situs lelang internet. Contoh Catatan penggunaan telpon.

1. **Memory imaging techniques**

* Crash Dumps

adalah sekumpulan data hasil analisa komputer dalam waktu singkat yang isinya berupa kumpulan informasi yang berhasil terkumpul saat suatu event error (lag/crash/freeze) terjadi.

* Firewire

merupakan salah satu metode transfer data antara perangkat digital, khususnya perangkat audio dan video.