

*Polinema 2017*

**POLICE LINE DO NOT CROSS POLICE**

# IT FORENSIK

TI4F

Nova Iufian sovie



# **pengertian**

IT Forensik merupakan ilmu yang berhubungan dengan **pengumpulan fakta** dan **bukti pelanggaran keamanan sistem informasi** serta validasinya menurut metode yang digunakan (misalnya metode sebab- akibat), di mana IT Forensik bertujuan untuk mendapatkan fakta-fakta objektif dari sistem informasi. Fakta-fakta tersebut setelah di verifikasi akan menjadi bukti-bukti yang akan di gunakan dalam proses hukum, selain itu juga memerlukan keahlian dibidang IT (termasuk diantaranya hacking) dan alat bantu (tools) baik hardware maupun software.





# tujuan

Tujuan dari IT forensik adalah untuk menjelaskan keadaan artefak digital terkini. Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM), dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan. Bidang IT forensik juga memiliki cabang-cabang di dalamnya seperti firewall forensik, forensik jaringan, database forensik, dan forensik perangkat mobile.



# Kejahatan komputer



## ***Komputer crime***

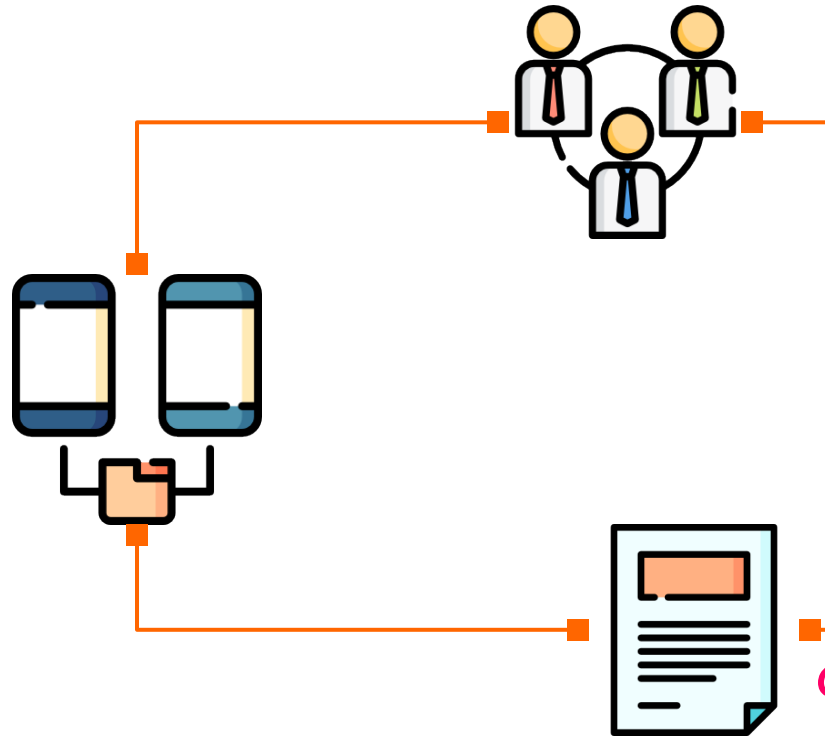
Merupakan kegiatan berbahaya dimana menggunakan media komputer dalam melakukan pelanggaran hukum.



## ***Komputer fraud.***

Kejahatan atau pelanggaran dari segi sistem organisasi komputer.

**perangkat**  
perangkat untuk  
kepentingan digital forensik  
dapat dibedakan kepada  
dua kategori yaitu  
hardware dan software



## **manusia**

pelaku yang mempunyai kualifikasi tertentu untuk mencapai kualitas yang diinginkan (*Collection Specialist., Examiner, Investigator* )

## **aturan**

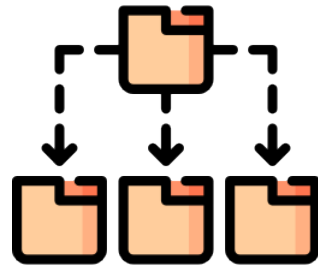
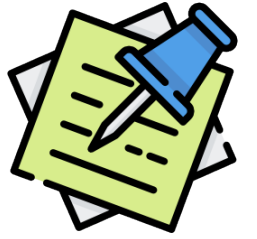
prosedur dalam mendapatkan, menggali, menganalisa barang bukti dan akhirnya bagaimana menyajikan hasil penyelidikan dalam laporan.



# komponen

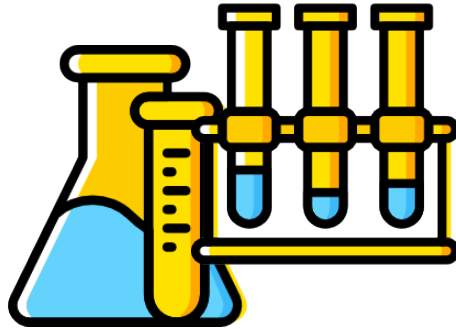


# tahapan



## ***Pengumpulan data***

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



## ***pengujian***

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



## ***analisis***

Tugas analisis ini mencakup berbagai kegiatan, seperti identifikasi user atau orang di luar pengguna yang terlibat secara tidak langsung, lokasi, perangkat, kejadian, dan mempertimbangkan bagaimana semua komponen tersebut saling terhubung hingga mendapat kesimpulan akhir.





## ***Dokumentasi dan laporan***

Dalam hal ini computer forensik memiliki peran yang sangat penting sebagai bagian dari upaya penyiapan bukti-bukti digital di persidangan.



## **contoh**

*Kasus ini berhubungan dengan artis Alda, yang dibunuh di sebuah hotel di Jakarta Timur. Ruby Alamsyah menganalisa video CCTV yang terekam di sebuah server. Server itu memiliki hard disc. Ruby memeriksanya untuk mengetahui siapa yang datang dan ke luar hotel. Sayangnya, saat itu awareness terhadap digital forensik dapat dikatakan belum ada sama sekali. Jadi pada hari kedua setelah kejadian pembunuhan, Ruby ditelepon untuk diminta bantuan menangani digital forensik. Sayangnya, kepolisian tidak mempersiapkan barang bukti yang asli dengan baik. Barang bukti itu seharusnya dikarantina sejak awal, dapat diserahkan kepada Ruby bisa kapan saja asalkan sudah dikarantina. Dua minggu setelah peristiwa alat tersebut diserahkan kepada Ruby, tapi saat ia periksa alat tersebut ternyata sejak hari kedua kejadian sampai ia terima masih berjalan merekam. Akhirnya tertimpalah data yang penting karena CCTV di masing-masing tempat/hotel berbeda settingnya. Akibat tidak aware, barang bukti pertama tertimpa sehingga tidak berhasil diambil datanya.*

**</ Terima kasih >**