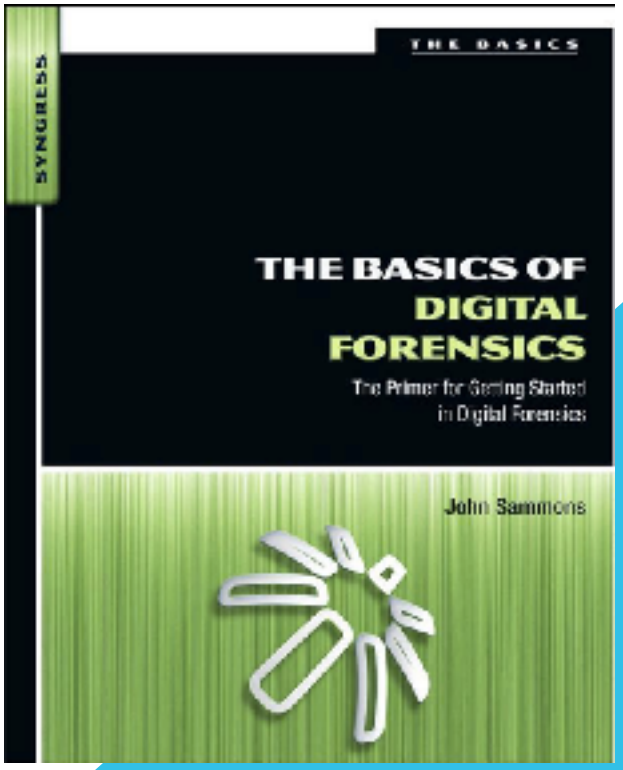


11. LOOKING AHEAD

TOPIK

- Standards and Controls
- Cloud Forensics
- Solid State Drives
- Speed of Change

STANDARD DAN KONTROL

- Standard
  - Sampel disiapkan yang memiliki sifat yang sudah diketahui yang digunakan sebagai kontrol selama analisis forensik
- Control
  - Tes dilakukan secara paralel dengan sampel eksperimental
  - Sampel yang memberikan hasil yang dikenal

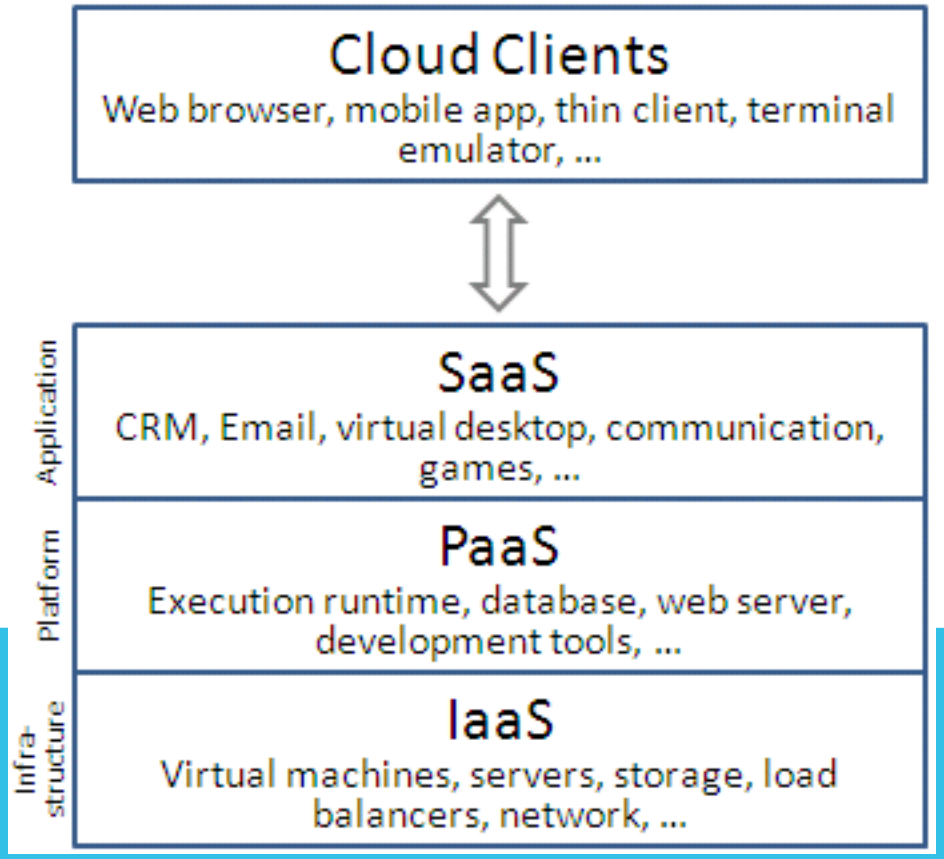
Beberapa otoritas forensik ingin menggunakan konsep-konsep ini dalam forensik komputer, yang lainnya tidak

CLOUD FORENSICS

CLOUD COMPUTING

- Infrastructure as a Service (IaaS)
- Software as a Service (SaaS)
- Platform as a Service (PaaS)

Image dari Wikipedia, Ch 11a: Cloud computing - Wikipedia



INFRASTRUCTURE AS A SERVICE (IAAS)

- Layanan cloud yang paling dasar
  - Seperti menyewa server fisik di fasilitas lokasi bersama
- Menyediakan mesin virtual dan layanan jaringan kepada pelanggan
- Customer menginstal OS & apikasi
  - Bertanggung jawab untuk memelihara dan mengupgrade OS & aplikasi
- Contoh: Amazon EC2, Azure Services Platform, Google Compute Engine, Rackspace Open Cloud

PLATFORM AS A SERVICE (PAAS)

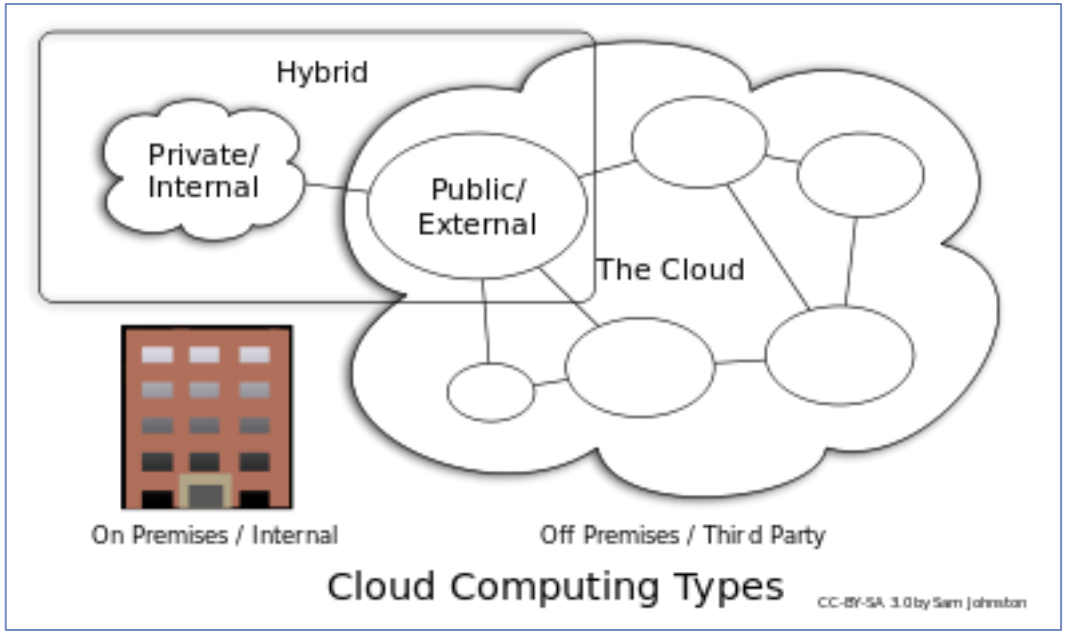
- Menyediakan platform komputasi yang mencakup
  - Sistem Operasi
  - Lingkungan eksekusi bahasa pemrograman
  - Database
  - Web server
- Pengembang aplikasi mendesain aplikasi tanpa mengelola layer hardware & software yang lebih rendah
- Contoh: AWS Elastic Beanstalk, Windows Azure Cloud Services, Google App Engine

SOFTWARE AS A SERVICE (SAAS)

- Menyediakan aplikasi untuk digunakan
- Klien tidak mengontrol hardware, OS, atau aplikasi
  - Mereka hanya menggunakan fitur aplikasi yang disediakan
- Contoh: Google Apps, Microsoft Office 365

PRIVATE DAN PUBLIC CLOUDS

- Private cloud
  - Perusahaan membeli dan memelihara server
  - Terbatas hanya untuk pengguna perusahaan
  - Menghilangkan banyak keuntungan dari komputasi awan
  - Lebih aman (?)
- Public Cloud
  - Jenis yang paling umum, yang disediakan oleh Amazon atau Microsoft, dll
- Image from Wikipedia, link
  Ch 11a: Cloud computing – Wikipedia



Comparison for SaaS

	Public cloud	Private cloud
Initial cost	Typically zero	Typically high
Running cost	Predictable	Unpredictable
Customization	Impossible	Possible
Privacy	No (Host has access to the data)	Yes
Single sign-on	Impossible	Possible
Scaling up	Easy while within defined limits	Laborious but no limits

- From Wikipedia, link Ch 11a: Cloud computing - Wikipedia

KEUNTUNGAN CLOUD

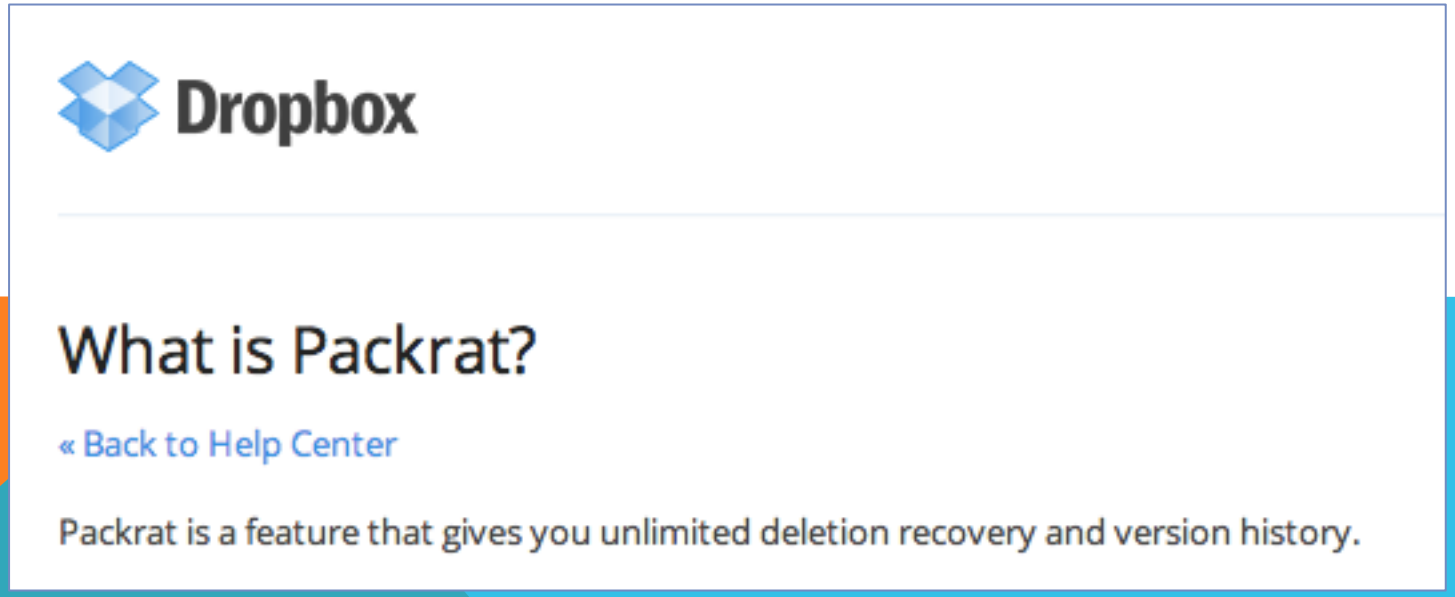
- Biaya Awal lebih rendah
- Flexibilitas
- Scalabilitas
- Redundancy
- Tugas pemeliharaan server menjadi tanggung jawab pihak lain sehingga bisnis dapat fokus pada kompetensi inti mereka

KEKHAWATIRAN HUKUM

- Biasanya tidak ada cara untuk memulihkan data yang dihapus
- Data yang dihapus berada pada penyimpanan bersama, dan mapping segera dihapus ketika file dihapus
- Sedikit tool forensik yang tersedia untuk lingkungan cloud

CLOUD PERSISTENCE: DROPBOX

- Dropbox menyimpan semua file yang di delete
  - Untuk home user defaultnya 30 hari
  - Selamanya dengan ekstension Packrat (default untuk bisnis users)
- Sangat berguna bagi para penyidik!
  - Link Ch 11b: Dropbox - What is Packrat?



YURIDIKASI (MASALAH HUKUM)

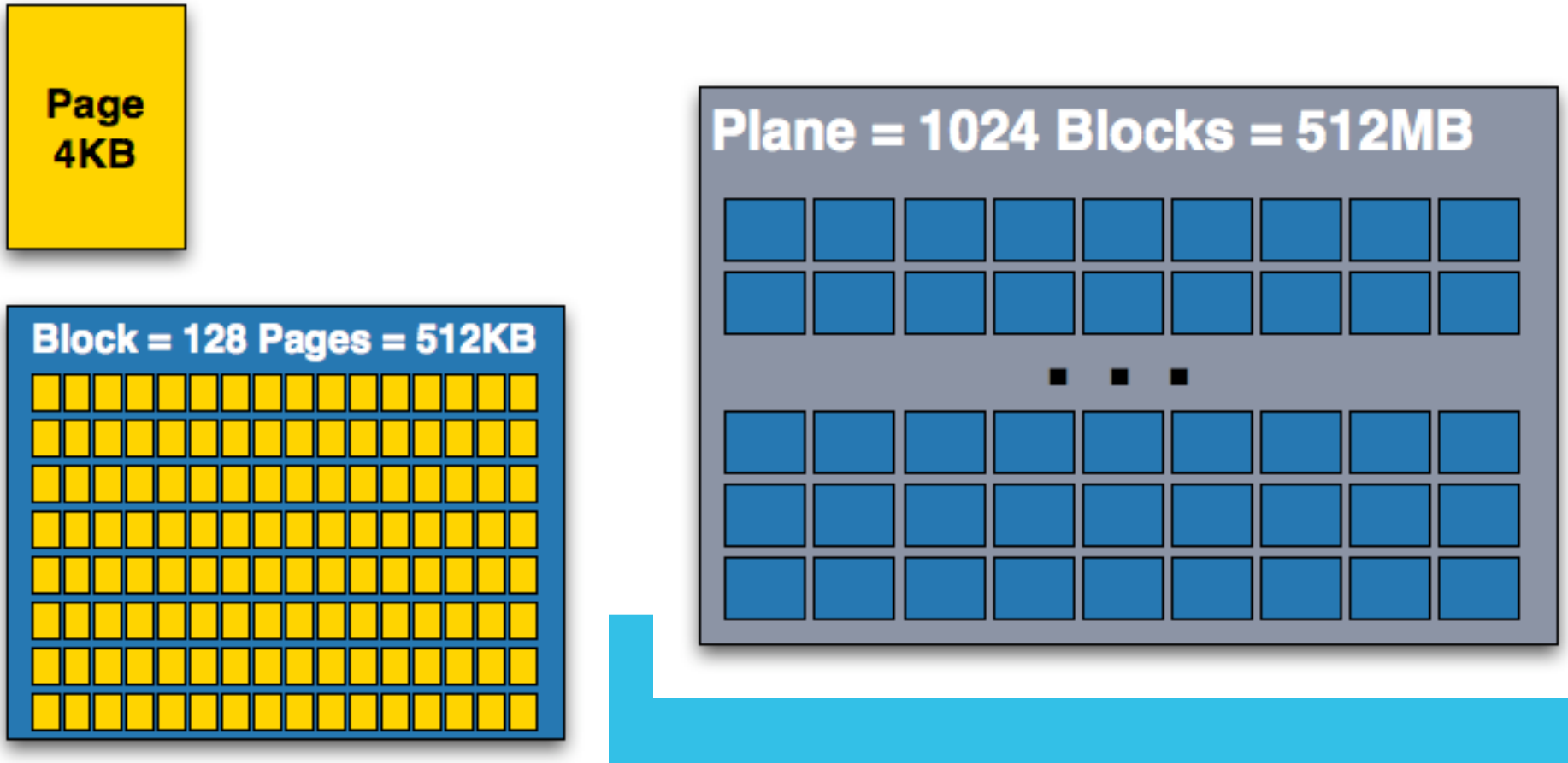
- Penyedia layanan cloud bisa berada di mana saja di dunia
- Peraturan bisa membantu, jika mereka diperlukan Penyedia Layanan Cloud untuk mempertahankan dan memberikan data kepada penyidik
- Service Level Agreements mencakup pengumpulan bukti digital dan perlindungan
  - Tindakan pencegahan yang tepat saat terjadi gugatan

SOLID STATE DRIVES

STRUKTUR INTERNAL SSD

Link Ch 11d: Internal Structure of an SSD

STRUKTUR SSD



Link Ch 11c: Understanding SSDs

SSDS DAN TRIM

- SSD menjadi lambat saat penuh
- Kecepatan SSD hanya cepat ketika SSD dapat ditulis secara parallel
- Struktur terkecil yang bisa ditulis adalah page (4 KB)
  - Tapi Anda tidak bisa menulis ke halaman kecuali itu kosong
- Struktur terkecil yang bisa dihapus adalah blok (512 KB)
- Juga, Anda hanya dapat menghapus blok 10.000 kali sebelum akhirnya gagal (setidaknya pada 2009)
- SSD tidak semua nya sama- mereka memiliki perbedaan untuk meningkatkan umur dengan ”umur pakai”

Link Ch 11e: SSD Myths and Legends - 'write endurance' article in StorageSearch.com

FILE TRANSLATION LAYER

- Komputer tahu di mana data yang akan disimpan pada drive
- SSD menggunakan file Translation Layer untuk memetakan lokasi ke lokasi sebenarnya
- Lokasi real disesuaikan dengan controller SSD untuk memakai perataan

Ch 11e: SSD Myths and Legends - 'write endurance' article in StorageSearch.com

GARBAGE COLLECTION

- Kontroler SSD menghapus file yang telah dihapus
- Ketika ini terjadi tergantung merek
- Data pada drive bahkan mungkin berubah selama akuisisi forensik
- Proses ini mungkin tergantung pada OS dan Format disk
- Perintah TRIM memungkinkan OS untuk memberitahu controller SSD bahwa file telah dihapus
- Didukung oleh Windows 7 dan OS X tetapi hanya aktif bila kondisi tepat

KECEPATAN PERUBAHAN

- Backlog kasus
- Update konstan perangkat lunak memerlukan metode baru, pelatihan dan penelitian
- Jaringan Profesional
  - HTCIA
  - Twitter
  - Conventions