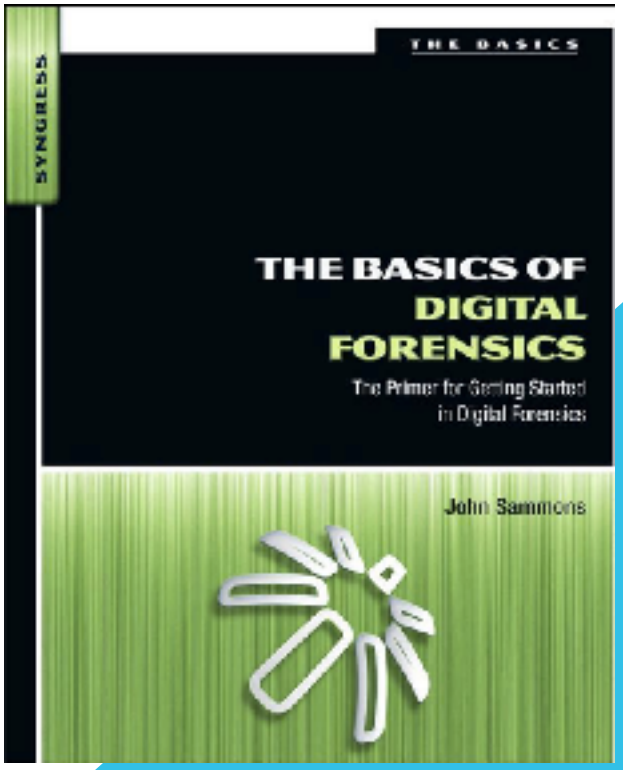


10. MOBILE DEVICE FORENSICS

PART 1

TOPICS

- Cellular Networks
- Cell Phone Operating Systems
- Evidence on Cell Phones

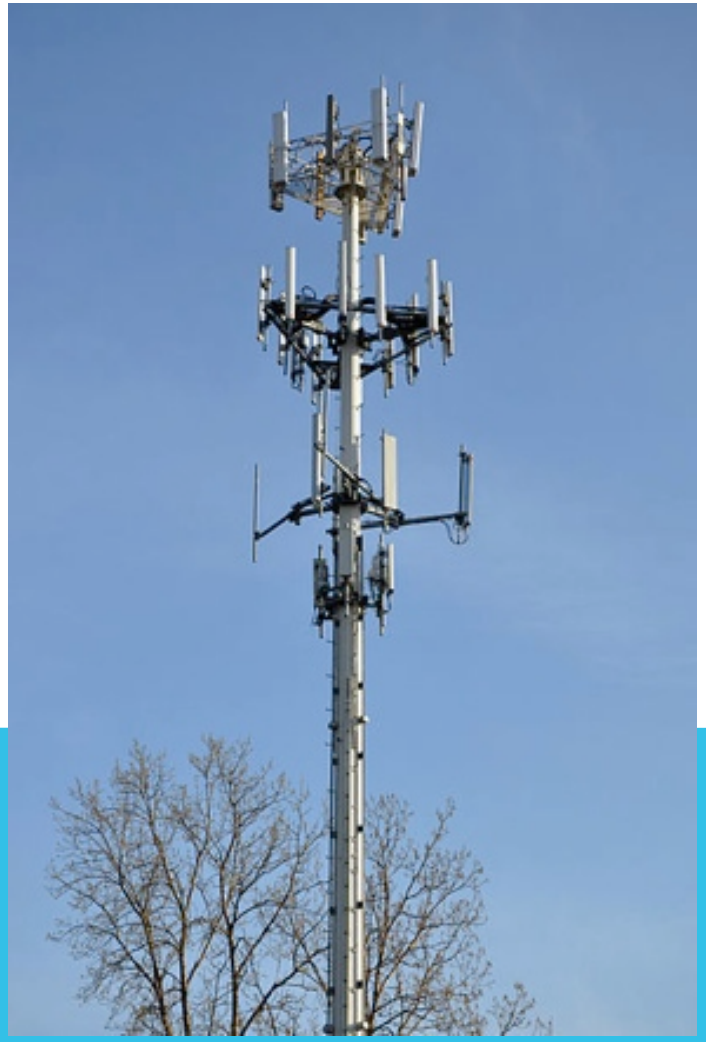
CELLULAR NETWORKS

CELL PHONE BASICS

- bukti penting
  - Emails & SMS messages
  - Internet history
  - GPS (Global Positioning System)
  - Photos
  - Videos
- Challenge: Keanekaragaman
  - Banyak merek, model, dan sistem operasi
  - Tidak ada antarmuka hardware standar
  - Kebanyakan menggunakan USB mini atau mikro USV

CELL PHONE TOWER

- Disebut juga “Base Transceiver Station” atau “Cell Site”
- Image from Wikipedia (Link Ch 10a: Cell site - Wikipedia)

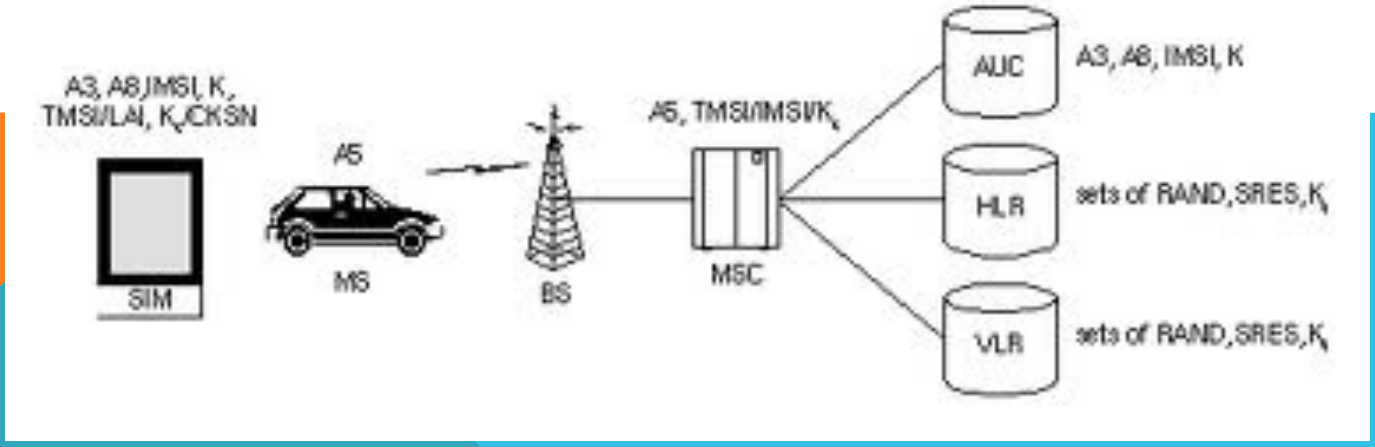


CELL NETWORK COMPONENTS

- Base Station
  - Antenna dan peralatan terkait
- Base Station Controller (BSC)
  - Mengatur sinyal antara base station
  - Penting saat ponsel berpindah dari satu tempat ke tempat
- Mobile Switching Center (MSC)
  - Memproses panggilan dalam jaringan
  - Menyimpan banyak bukti
  - Mengatur panggilan antara jaringan wireless dan land line yang berbeda
  - Menangani pesan SMS
  - Catatan detail panggilan dan log tersimpan di sini

CELL NETWORK COMPONENTS

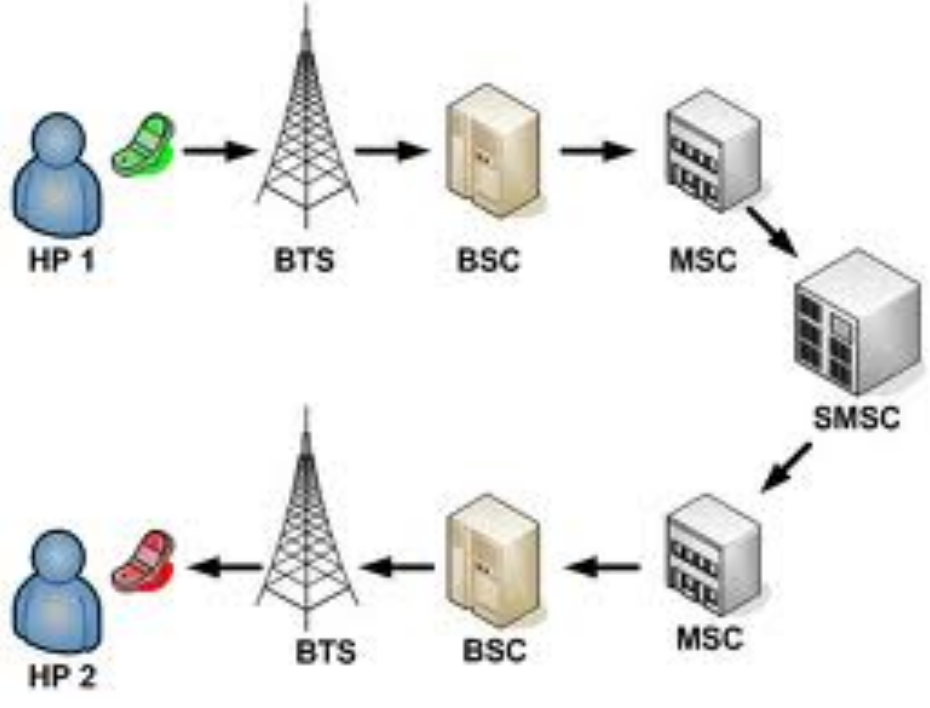
- Visitor Location Register (VLR)
  - Database terkait dengan MSC
  - Semua perangkat mobile saat ini sedang dikendalikan menggunakan MSC yang dicatat dalam VLR
  - Fungsi interworking adalah sebagai gateway ke jaringan data luar seperti Internet
- Home Location Register (HLR)
  - Informasi tentang pelanggan individu
  - ID, billing, and services
  - Menyimpan kunci enkripsi
  - Mendukung Authentication Center (AuC) yang mengontrol akses ke jaringan



CELL NETWORK COMPONENTS

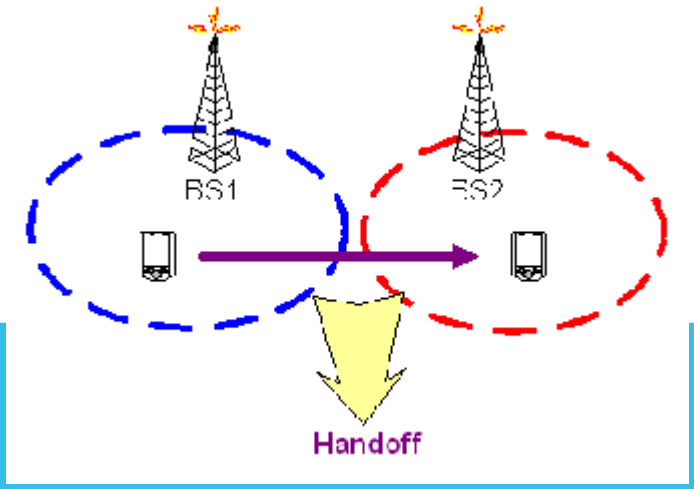
Short Message Service Center (SMSC)

- Bertanggung jawab untuk pesan SMS
- Pesan bisa direcover
- Tidak ada aturan yang mengatur berapa lama provider harus menyimpan pesan-pesan sms



HANDOFF

- Setiap ponsel secara teratur berkomunikasi dengan tower seluler terdekat
- Bahkan jika ponsel tidak digunakan
- Ia mengirimkan data identifikasi ke menara
  - Nomor ponsel dan penyedia layanan
- Handoff adalah perpindahan dari tower ke tower saat Anda bergerak



HANDOFF

- Ditangani secara berbeda pada jaringan GSM & CDMA
  - GSM (Global System for Mobile Communication)
    - Hard handoff: Ponsel hanya dapat terhubung ke satu tower pada suatu waktu
  - CDMA (Code Division Multiple Access)
    - Soft handoff
    - Ponsel bisa terkoneksi ke beberapa tower pada satu waktu
- Rekaman yang menampilkan kapan ponsel terhubung ke tower dapat digunakan untuk menentukan perkiraan lokasi ponsel

MOBILE SWITCHING CENTER (MSC)

- Saat panggilan Anda mencapai tower maka panggilan diteruskan ke MSC
- Jika saat Anda menelepon telepon berada di luar jaringan, panggilan akan diteruskan ke PSTN (Public Switched Telephone Network)

MESSAGING SERVICES

- SMS (Short Message Service)
  - Text messages
  - Maximum 160 karakter
- MMS (Multimedia Messaging Service)
  - Fungsinya disempurnakan
  - Tidak ada batasan 160 karakter

JENIS JARINGAN CELLULAR

- CDMA (Code Division Multiple Access)
- GSM (Global System for Mobile Communications)
- iDEN (Integrated Digitally Enhanced Network)

CDMA (CODE DIVISION MULTIPLE ACCESS)

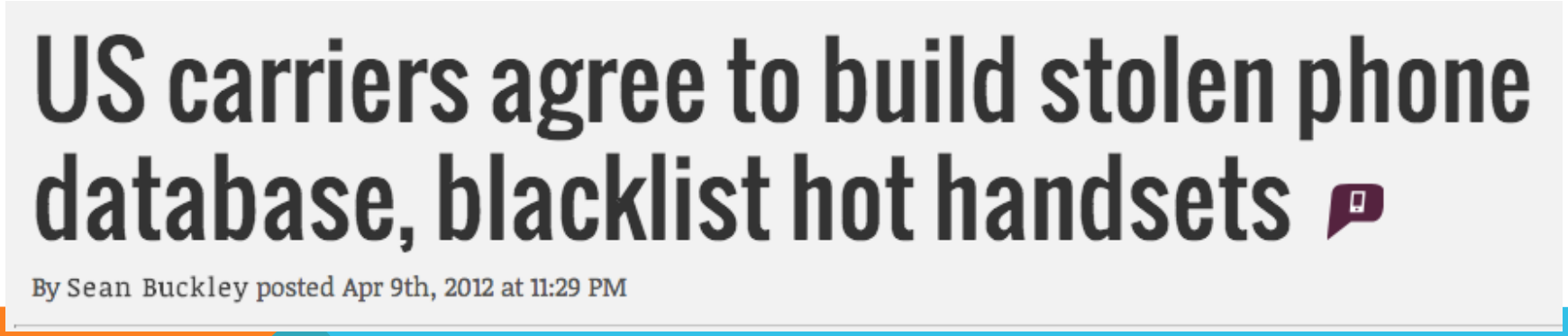
- Awalnya teknologi militer
- Menggunakan spread spectrum
- Digunakan oleh Sprint, Verizon, Alltel, and NEXTEL
- Tidak menggunakan kartu SIM (Subscriber Identity Module)
- Ponsel diidentifikasi oleh Electronic Serial Number (ESN)
  - ESNs memiliki 32 bit dan tidak lagi digunakan sejak 2010, dan digantikan sistem baru, MEID
  - MEID memiliki 56 bit (Link Ch 10b: Electronic serial number - Wikipedia)

GSM (GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS)

- digunakan secara internasional
- Menggunakan Time Division Multiple Access (TDMA)
- Menggunakan kartu SIM (Subscriber Identity Module)
- Operator termasuk AT & T, Verizon, T-Mobile dan Cellular One
- Ponsel diidentifikasi oleh International Mobile Equipment Identity (IMEI) nomor (15 atau 16 digit)

IMEI BLACKLIST

- IMEI bersifat unik mengidentifikasi telepon, dan tidak berubah dengan mengganti kartu SIM
- IMEI dapat digunakan untuk memblacklist telepon yang dicuri
  - Links
  - Ch 10c: International Mobile Station Equipment Identity - Wikipedia
    Ch 10d: US carriers agree to build stolen phone database, blacklist hot handsets



US carriers agree to build stolen phone database, blacklist hot handsets

By Sean Buckley posted Apr 9th, 2012 at 11:29 PM

IDEN (INTEGRATED DIGITALLY ENHANCED NETWORK)

- Seperti fungsi radio dua arah
- Mendukung pengguna telepon normal dan pengiriman "push-to-talk“ pengguna
- Sprint akan berhenti mendukung iDEN pada bulan Juni, 2013
  - Link Ch 10e: Integrated Digital Enhanced Network - Wikipedia

PREPAID CELL PHONES

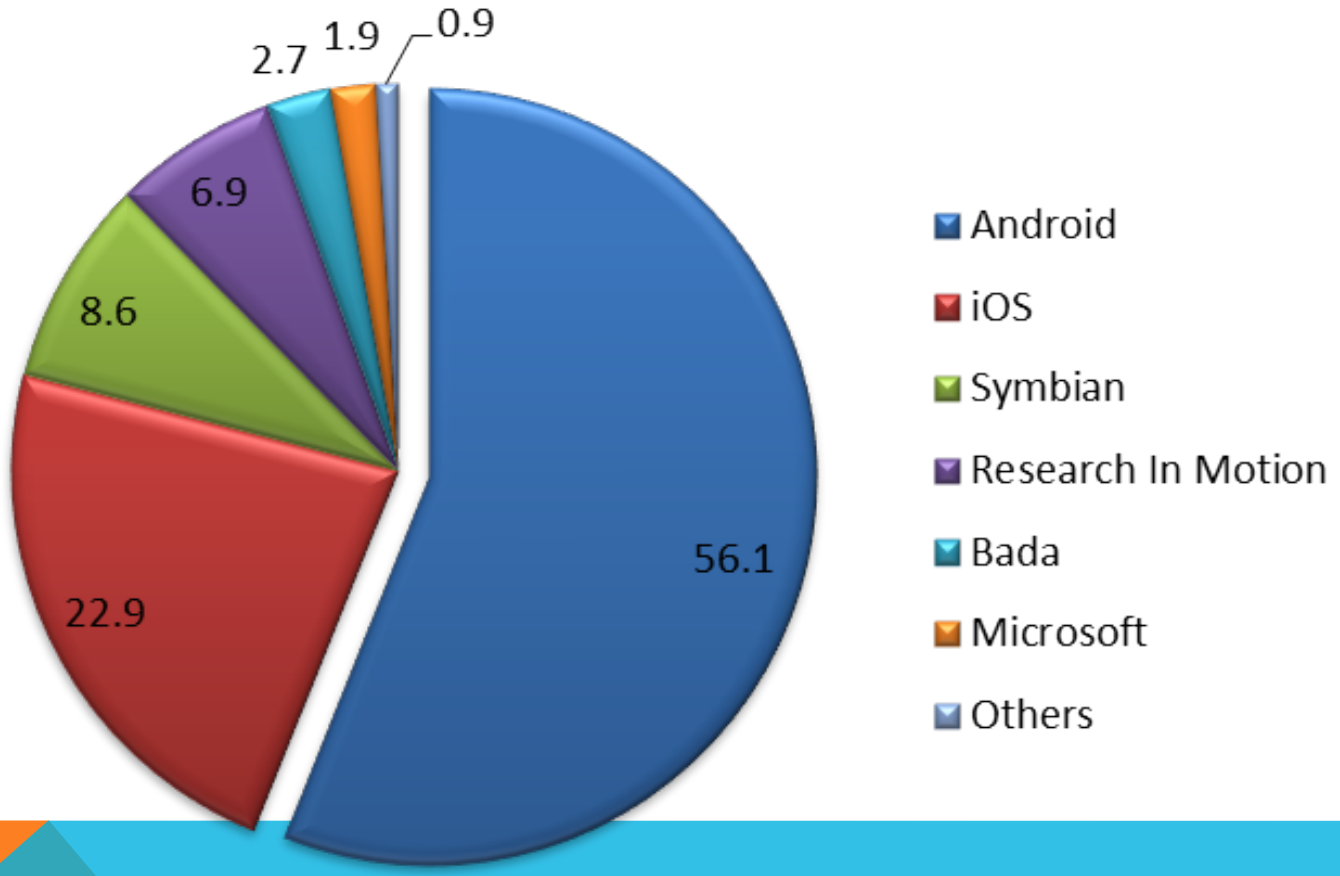
- Bisa dibeli dengan uang tunai
- Tidak ada jejak untuk mengidentifikasi identitas pengguna
- Ponsel akan menyimpan informasi pelanggan
- Penyedia jaringan hanya akan memiliki rincian panggilan
  - Lokasi dan panggilan yang dikirim dan diterima

SISTEM OPERASI PONSEL

SISTEM OPERASI PONSEL MODERN

- Symbian
- Apple iOS
- Windows CE and Windows Mobile
- Google’s Android
- Blackberry OS

Mobile OS Market Share - 1Q2012



Link Ch 10f: Mobile OS Market Share

SYMBIAN

- Diawali sebagai EPOC pada tahun 1980 an
- Pertama kali digunakan pada ponsel pada tahun 2000 oleh Sony
- Melewati banyak perusahaan yang berbeda
- Nokia baru-baru ini membuat open-source
- Pada tahun 2011, Nokia beralih ke Windows Phone
- Accenture terus mendukung Symbian

BLACKBERRY

- Diperkenalkan pada tahun 1999 oleh Research In Motion (RIM) dari Kanada
- Umum di tempat kerja
- Sinkronisasi dengan Novell GroupWise dan Microsoft Exchange
- OS versi yang berbeda untuk masing-masing operator

Barack Obama's BlackBerry 'no fun'

Barack Obama fought hard to keep his BlackBerry when he became president, but with only 10 people authorised to email the super-encrypted device, he admitted that it is "no fun."

Barack Obama used his BlackBerry extensively during the 2008 Presidential campaign Photo: AFP

Barack Obama

News » World News »
North America »
USA »

In Barack Obama

Link [Ch 10h: Barack Obama's BlackBerry 'no fun'](#)

ANDROID

- OS Yang paling populer OS sejauh ini
- Open Source
- Digunakan pada Motorola, Sony Ericsson, dan ponsel HTC
- Juga pada tablet

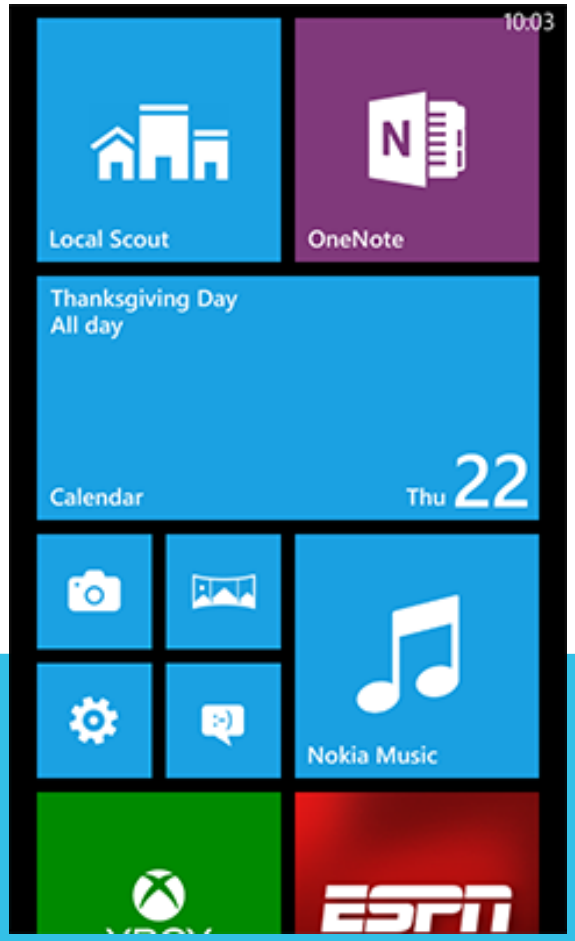
APPLE'S IOS

- Digunakan pada iPhone, iPad, dan iPod Touch
- Berdasarkan OS X
- OS ponsel kedua yang paling populer

WINDOWS MOBILE (NOW WINDOWS PHONE)

- Versi OS Windows untuk smartphone dan pocket PC
- Windows Phone 8 dirilis pada Oktober 2012

- Link Ch 10i: Windows Phone - Wikipedia



BARANG BUKTI PADA PONSEL

ITEM BARANG BUKTI POTENSIAL

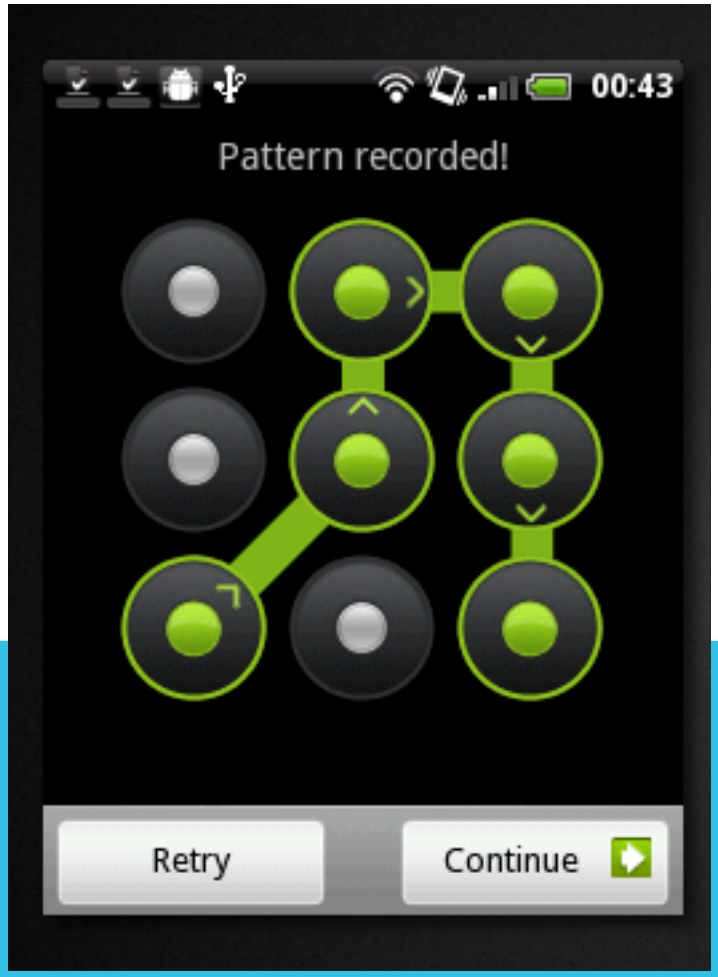
- Call history
- Text messages (active & deleted)
- Email
- Photos & video
- Browser history
- Contacts
- GPS location information
- Chat sessions
- Calendar
- Voice memos
- Dokumen

PIN
(PERSONAL IDENTIFICATION NUMBER)

- Dapat digunakan untuk mengamankan handset
- Tiga kali gagal akan mengunci SIM
- Personal Unlock Key (PUK) dibutuhkan untuk unlock SIM
  - PUK berasal dari penyedia kartu SIM

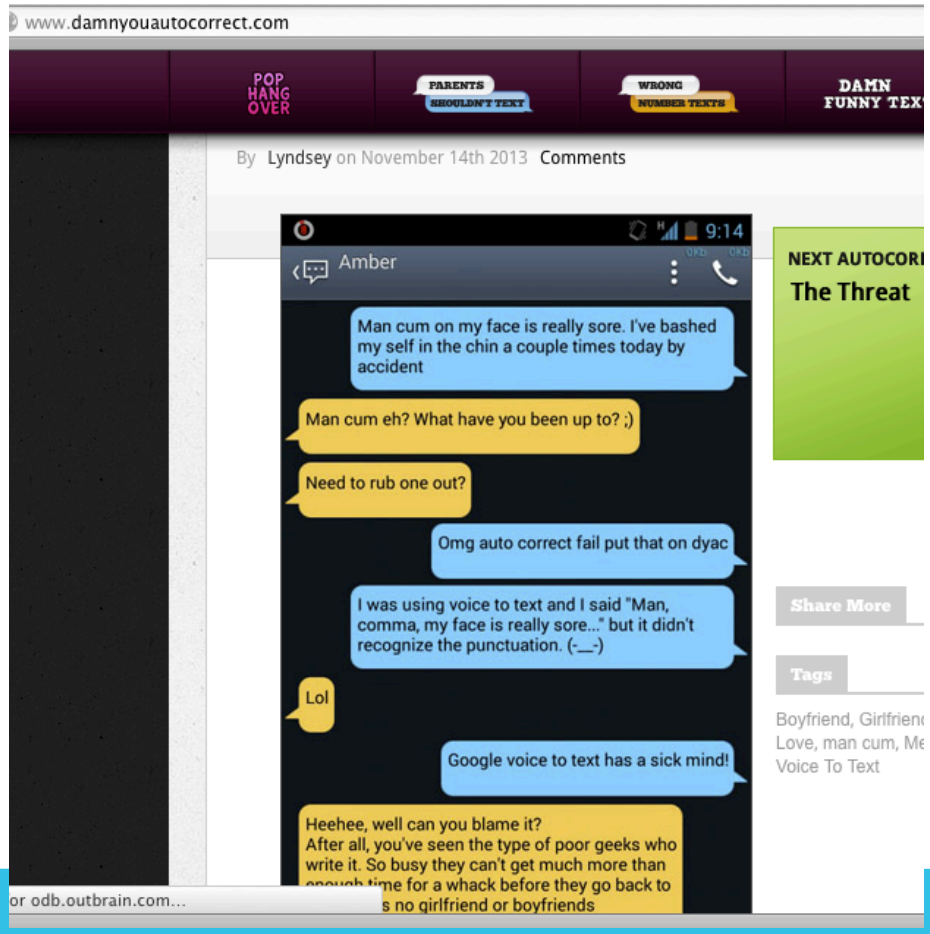
gambar dari link

Ch 10j: How to Secure Your Android Phone



PREDICTIVE TEXT

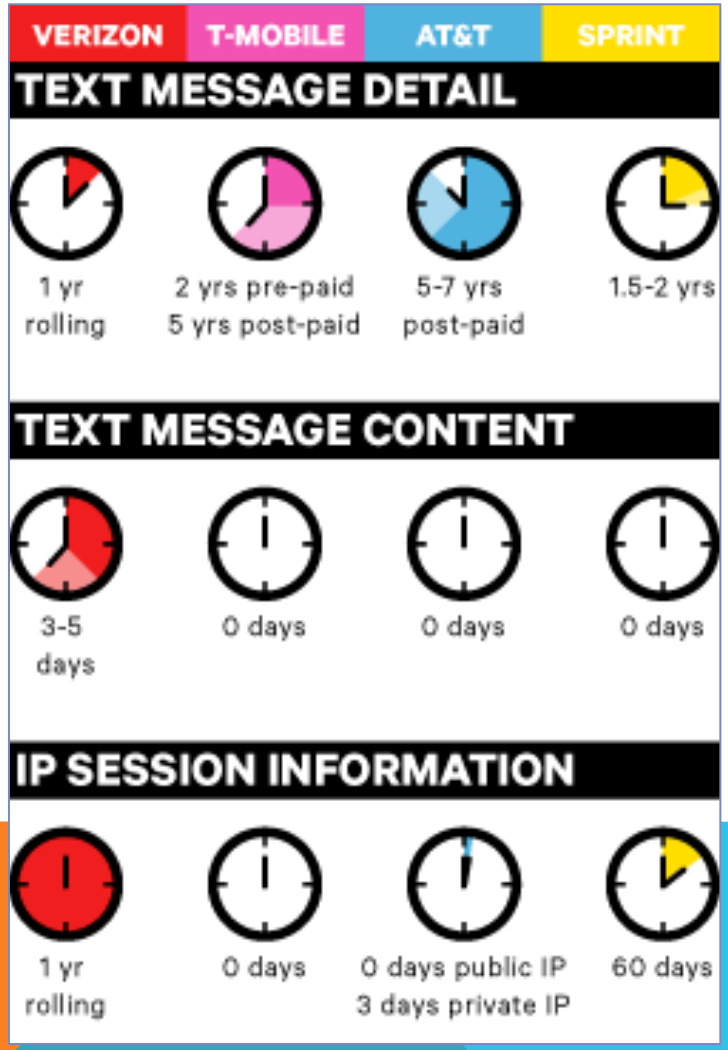
- Dimaksudkan untuk mempermudah mengetik pada keypad 10 digit
- Mengisi teks ketika pengguna mengetik bagaian kata
  - Sistem belajar kata-kata yang sering digunakan
  - Database dapat berisi kata-kata, bahasa gaul, singkatan, alamat e-mail atau URL
- Kadang-kadang membuat pesan menjadi kacau
  - Link Ch 10k: Damn You Auto Correct!

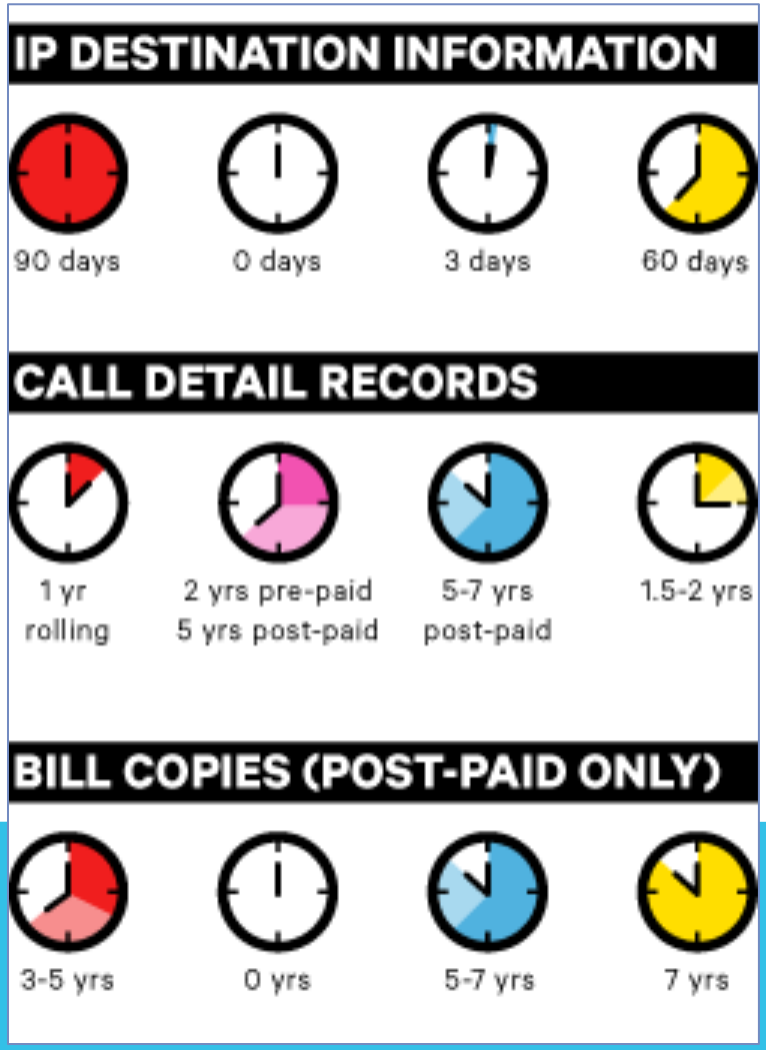


CALL DETAIL RECORDS (CDR)

- Digunakan oleh operator untuk memecahkan masalah dan meningkatkan kinerja
- Mungkin menunjukkan:
  - Tanggal / waktu panggilan mulai dan berakhir
  - Siapa yang menelepon siapa
  - Apakah panggilan itu masuk atau keluar
  - asal dan akhir tower
- Tapi Anda tidak bisa mengatakan siapa yang memegang telepon
- Informasi pelanggan berbeda dengan CDR
  - Name, address, acct. numbers, email address, credit card #

KEBIJAKAN PENYIMPANAN





Link [Ch 10I: Which Telecoms Store Your Data the Longest? Secret Memo Tells All]

- Perangkat lunak yang disertakan dalam ponsel untuk mengirim data pelacakan kembali ke pembawa
- kontroversi Privasi

(Link Ch 10m: Carrier IQ: What it is, what it isn't, and what you need to know)

MENEMUKAN CELL PHONES

Triangulation

- Mengukur sinyal delay sampai tiga menara terdekat
- Dapat memberikan perkiraan lokasi ponsel

Directional antenna

- Memungkinkan penentuan lokasi dengan hanya dua tower dari pengukuran delay

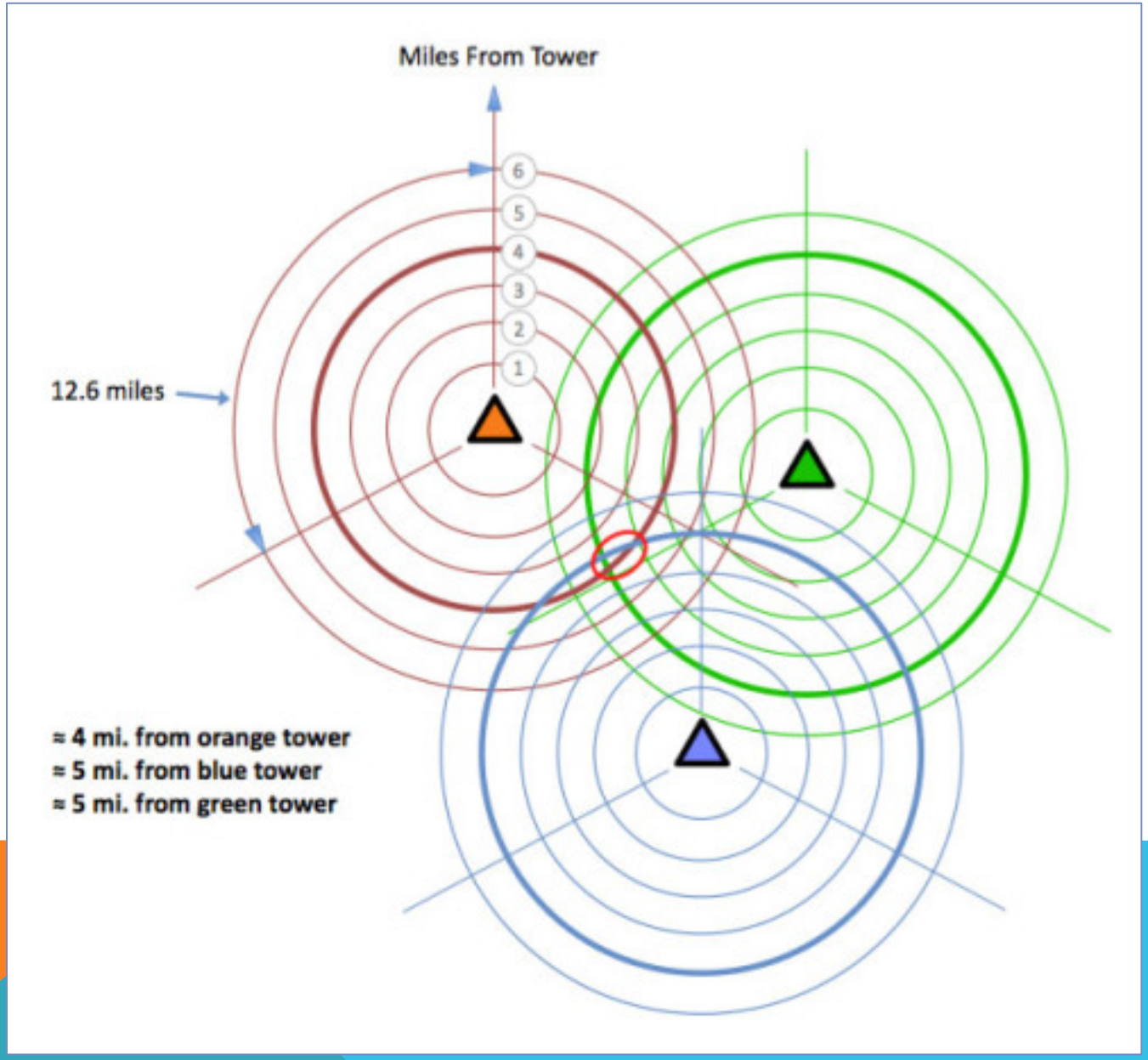
GPS

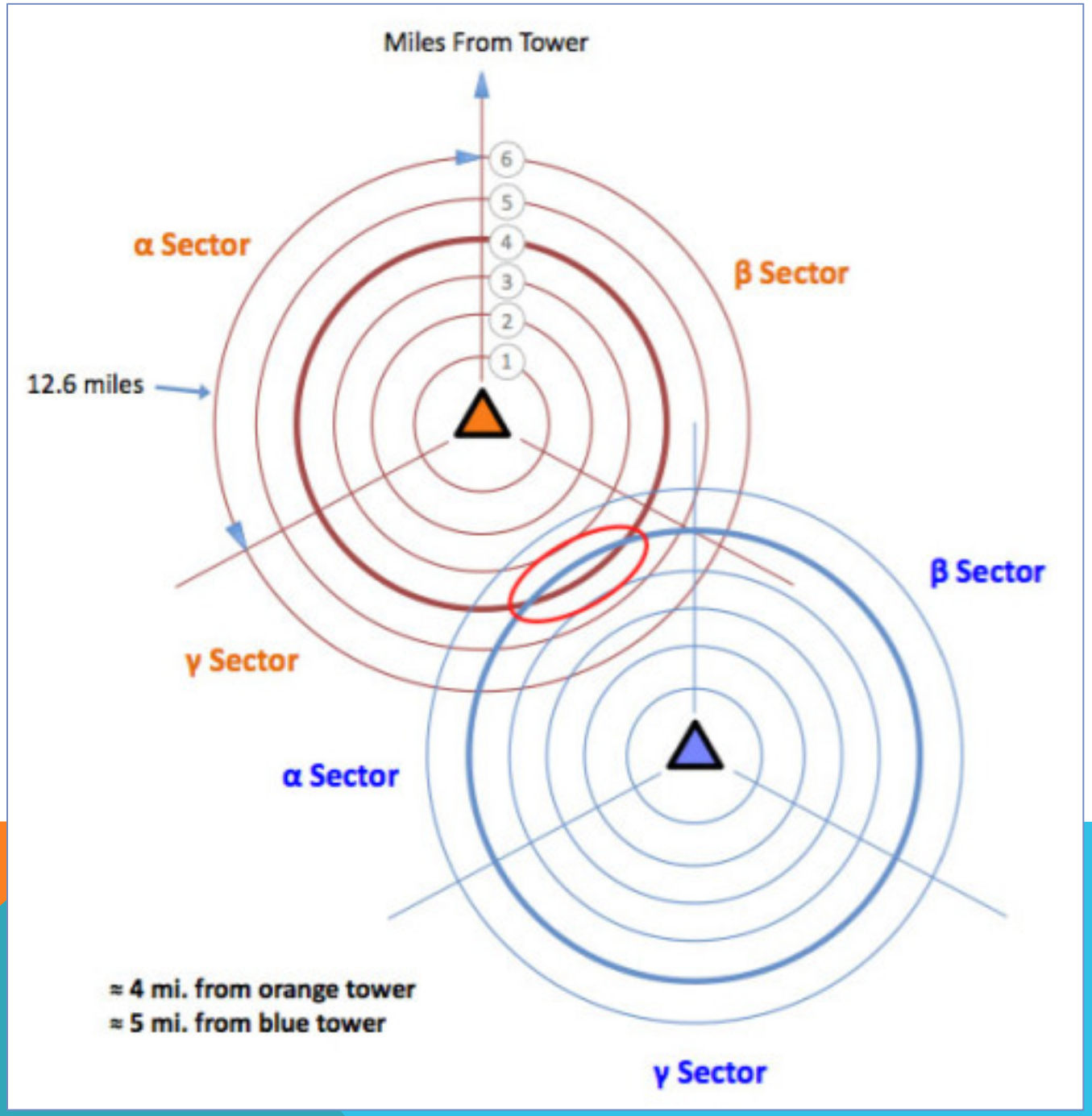
- Menenetukan posisi ponsel dengan satelit

Wi-Fi Positioning System

- Menggunakan data pada titik akses Wi-Fi yang diketahui
- Termasuk iPad

Link Ch 10n: Wi-Fi positioning system - Wikipedia


Miles From Tower
6
5
4
3
2
1
12.6 miles
≈ 4 mi. from orange tower
≈ 5 mi. from blue tower
≈ 5 mi. from green tower


Miles From Tower
6
5
4
3
2
1
α Sector
β Sector
12.6 miles
γ Sector
β Sector
α Sector
≈ 4 mi. from orange tower
≈ 5 mi. from blue tower
γ Sector

Triangulation images from link Ch 10o: Cell Tower Triangulation – How it Works