



Tajne računalne forenzike

CIS FER 2013

Damir Delija
Dr.Sc.E.E

Plan predavanja

- Cilj prezentacije
 - dati pregled što je računalna forenzika i kakvo je stanje
- Proći će se kroz
 - što je računalna forenzika
 - reakcije na incidente i računalna forenzika
 - alati, komercijalni i open source
 - primjene i uvođenja alata u postojeće velike sustave

Razvoj računalne forenzike

- Dva su osnovna motiva razvoja
 - razvoj računalnih znanosti
 - razvoj računalnih incidenata tj užem smislu računalni kriminal (uvijek vodi ...)
- Kao grana računalna forenzika relativno nova, ali postupci su tu od prvih dana korištenja računala (jedan od najranijih slučajeva Moris worm 1988)
- Metode računalne forenzike rade i za debugging sustava
 - pouzdano znati što se i kako desilo

Računalna forenzika

“Computer Forensics is simply the application of computer investigation and analysis techniques in the interest of determining potential legal evidence”

Judd Robbins

- To je primjena znanstvene (forenzičke) metode
- Dugotrajan, pedantan, dosadan postupak
- PS: Zaboravite seriju CSI.....

Računalna forenzika

- Cilj računalne forenzike je da prikaže i objasni stanje stanje digitalnih artefakata.
- Digitalni artefakti mogu biti
 - računalni sistem,
 - storage media,
 - elektronički dokument,
 - niz paketa u kretanju po mreži ...
- Objašnjene može biti jednostavno poput "koje su informacije pristune" " ili detaljno i sofisticirano kao "koji je niz događaja doveo do zatečenog stanja"

Zahtjevi na postupak računalne forenzike

- Postupak mora biti dobro dokumentiran i rezultati moraju biti ponovljivi
- Princip "najbolji dokazni materijal" tj. analiza se radi na egzaktnoj kopiji a ne živom sustavu – ako je ikako moguće
- Lanac kontrole dokaza (Chain of custody) mora garantirati pouzdanost dokaza
- **izuzetno važno - za sve mora postojati zapis/opis**

Legalni kriteriji

Da bi forenzička tehnika bila legalno prihvatljiva

- Da li je tehnika i postupak pouzdano testiran
- Da li je tehnika i postupak objavljen, provjeren od znanstvene zajednice
- Da li se pouzdano zna koja je vjerojatnost greške tehnike ili postupka
- Da li je tehnika i postupak prihvaćena od znanstvene zajednice.

Koraci forenzičkog postupka

Priprema : priprema alata i opreme potrebne za forenzički postupak;

Prikupljanje : prikupljanje dokumenta, logova, datoteka i izrada kopija fizičkih objekata koji sadrže elektroničke dokaze

Ispitivanje dokaza : izdvajanje dokaza iz prikupljenog materijala

Analiza : analiza dokaza prikupljenih u koraku ispitivanja dokaza

Izvještavanje : izrada izvještaja o nalazima

Računalna forenzika - obzirom na obuhvat sustava

- Forenzika mobilnih uređaja
 - profilira se kao posebno područje
- Forenzika pojedinačnog računala (host based)
 - najčešći slučaj - analize radne stanice
 - ulazi i forenzika aplikacije, uređaja
- Mrežnu forenziku (network enabled, system forensic)
 - analiza sustava kao umrežene cjeline, analiza sustava na razini mreže, analiza prometa na mreži, upravljanja mrežom
- Forenzika logova sustava (system log forensic)
 - rad sa zapisima – posebna nauka i alati

Forenzika sustava

- Mrežna forenzika (network enabled, system forensic)
 - analiza sustava kao umrežene cjeline,
 - analizu sustava na razini mreže,
 - analizu prometa na mreži, upravljanja mrežom
 - analiza aplikacija
- Danas svaki puta live forensic
 - Agent / servlet
 - Pasivni nadzor

Forenzika živog sustava

- Live forensic - analiza aktivnog uređaja ili sustava čiji se rad ne smije prekidati
- Najčešća na sustavima i sve češća u host forensic
- Radi se i na pojedinačnim uređajima i skupinama
- Postoji način na koji se na forenzički prihvatljiv način bilježe stanja uređaja
 - Agent / servlet
 - Pasivni nadzor

Standardni koraci računalne forenzike za računalne sustave

- Pokretanje **dokumentiranog** opisa incidentnog događaja u sustavu
- Identificiranje i kontrola incidenta
- Izrada i pohrana datoteka sa elektroničkim dokazima u lancu odgovornosti o dokazima
- Oporavak usluga i vraćanje / rekonstrukcija obrisanih podataka
- Prikupljanje i klasificiranje metadeta podataka po vremenu
- Povezivanje svih informacija o događajima u lanac događaja na osnovi vremena
- Analiza metadeta timelinea
- Dokumentiranje cijelog forenzičkog procesa i izvještavanje
- *Korištenje rezultata u daljim koracima*
 - *Detaljna analiza ključnih podatka iz forenzičkog izvještaja*
 - *Sudjelovanje u revizijama*

Računalna forenzika - po pristupu

- Proaktivna računalna forenzika
 - to je primjena metoda računalne forenzike na zdravom sustavu za dobivanje "baseline" (potpisa) sustava
- Retroaktivna računalna forenzika (klasična forenzika)
 - to je primjena nakon događaja – klasični post mortem
 - ide i bez proaktivne ali puno manja efikasnost

Preduvjet za forenziku je kvalitetna računalna administracija sustava (tj. pripremljen teren za rad)

Rezultat forenzičkog postupka - završno izvješće o incidentu

- Završno izvješće o incidentu
 - sadrži relevantne podatke o incidentu
 - sadrži opis postupka
- Informacije iz tog izvješća moraju omogućiti:
 - prepoznavanje izvora događaja;
 - prepoznavanja i uklanjanje sigurnosnih propusta
- Koristi se u sklopu procesa za upravljanje sigurnosnim incidentima

Računalna forenzika kao dio procesa kontrole incidenata i kao dio procesa nadzora sustava

Alati i ekspertiza

- Postoje alati za forenziku računalnog sustava na nivou operacijskog sustava i sklopovlja
- Ekspertiza vrlo rijetka
- Što se više ulazi u neku specifičnu granu to je situacija gora
- Dvije glavne grane ekspertize
 - Akademska – open source /UNIX oriented
 - Istražiteljska –law enforcement oriented

Komercijalni alati ili Opensource

- Nema idealnog alata
 - može postojati zahtjevani alat!
- Prednost sa pravne strane na komercijalnim alatima
- Opensource dodatni / kontrolni
- Filozofija odabira alata ista kao i za druge korporativne sustave
 - ključno je što mislite raditi i kako, u vašem sustavu

Alati

- EnCase guidance software
- FTK
- SleuthKit
- Helix CD
- The Coroner's Toolkit (TCT)
- Mnogi drugi

Primjene i uvođenja u postojeće sustave

- Primjene i uvođenja u postojeće velike sustave
 - dio incident responsa (IR)
 - dio preventivne pripreme i normalnog funkcioniranja sustava
- Samo novi pogled na stare prokušane tehnike kontrole sustava
 - dobra administracija sustva
- Dio pripreme za nastavak poslovanja
 - bitno razumjevanje važnosti metoda forenzike

Uloga u IT sustavima - područja

- Forenzika baza podataka
- Forenzika aplikacija / poslužitelja
- Forenzika logova / zapisa
- Forenzika mrežne opreme
- Forenzika multimedije (IP telefonija)
- Forenzika Scada sustava – procesno /industrijsko upravljanje
- Forenzika mobilnih uređaja i sustava
- Forenzika ugrađenih sustava
- Forenzika osobnih računala

Forenzika baza podataka

- Nema namjenskog alata
- Ekspertiza jako rijetka
- Sustavi složeni, velika količina podataka, visoka raspoloživost
 - zgodno znati svaki podatak ima cca 11 kopija negdje u sustavu
- Incidenti ostaju u kući
- Izvještaj od Verizona

"2008 DATA BREACH INVESTIGATIONS REPORT
Four Years of Forensic Research. More than 500
Cases. One Comprehensive Report"

Forenzika scada sustava

- Orgormna važnost energetika, industrija ...
- Danas - forenzika windows platforme i scada aplikacije
- Nekada - forenzika namjenskog uređaja
- Kompleksna okolina u pravilu loše administrirana
 - računalno nije primarno

Forenzika mobilnih uređaja

- Malo namjenskih alata
 - Neutrino
- Mali postotak podržanih uređaja
- Crne i sive metode (kloniranja ...)

Forenzika mrežnih uređaja

- Nema namjenskih alata
- Live forensic i forenzika logova

Područja računalnih znanja

Operativni sistemi

windows, linux, mac, unix,

Hardware

intel, mobilni uređaji, sparc, powerpc, scada
sustavi, embeded sustavi

Aplikacije

ono što korisnici koriste sa i bez svog znanja

Mreža, mrežni servisi i usluge

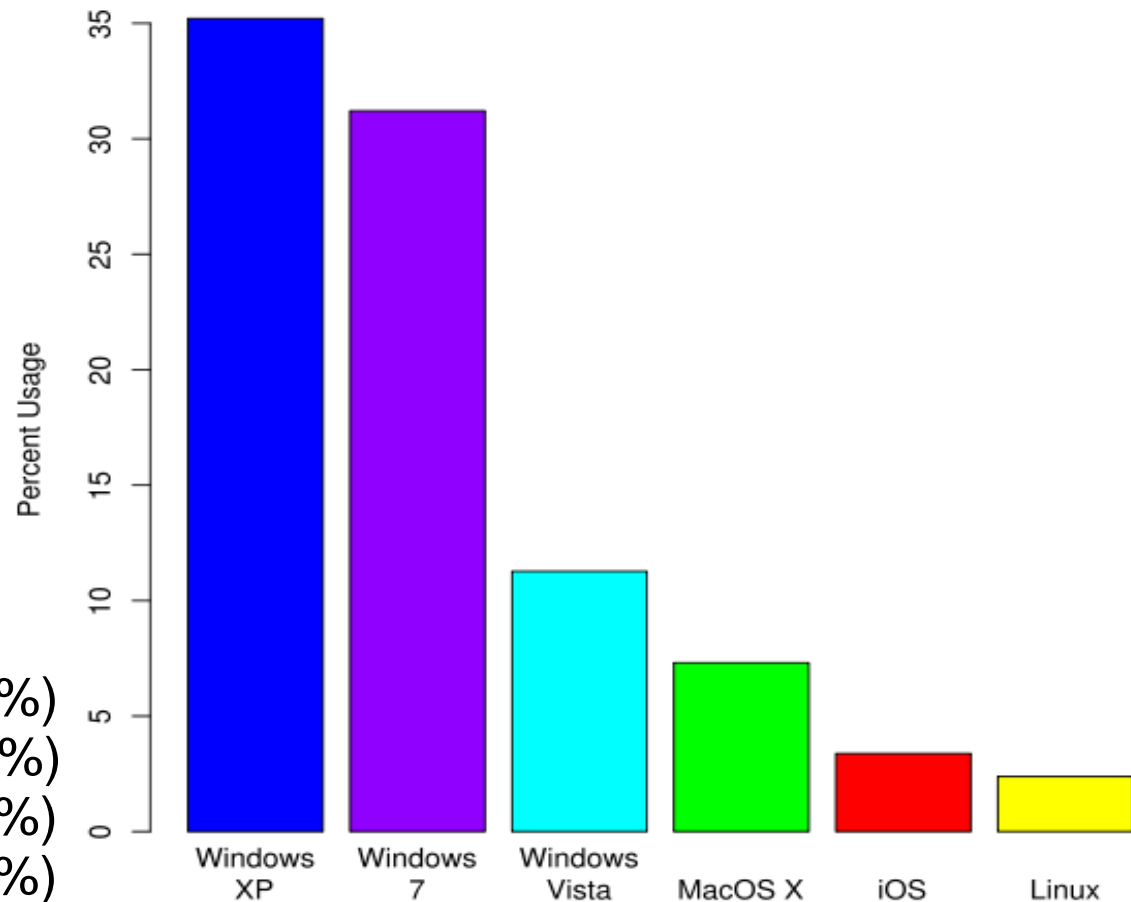
Operativni sistemi - korisnički

Windows ~ 75%

Linux ~ 3%

Mac ~ 12%

Usage share of web client operating systems: August 2011



Windows XP	(35.21%)
Windows 7	(31.21%)
Windows Vista	(11.27%)
Mac OS X	(7.31%)
iOS	(3.38%)
Android Linux	(1.30%)
GNU/Linux	(1.11%)

MS Windows

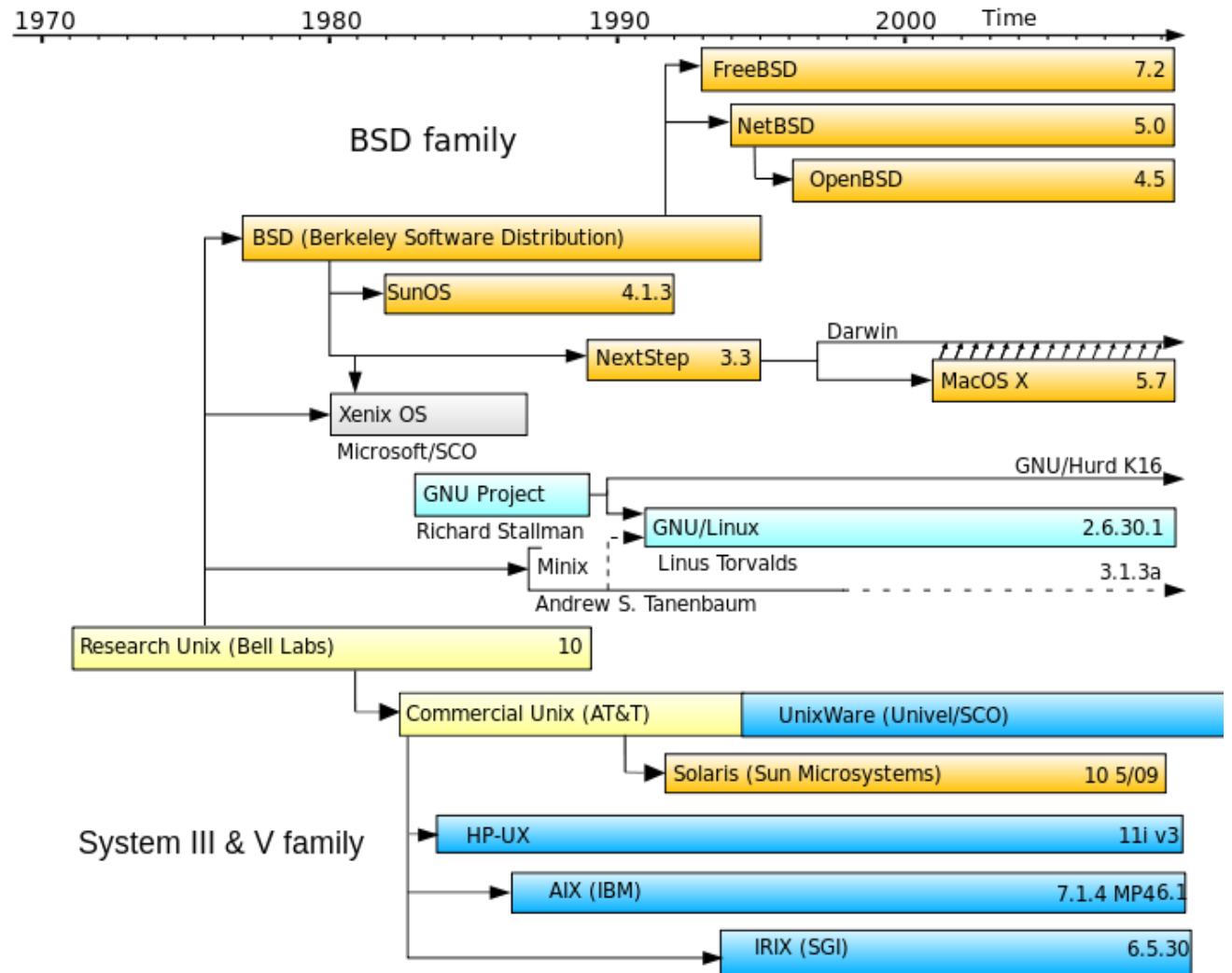
- win 3.11
- win nt, win 95, win 98,
- win2000
- win XP, win 2003
- vista
- win 7, windows 2008
- win 8
- windows mobile, windows ce

Svaka verzija ima specifičnosti

- drugačija struktura direktorija
- drugačija pohrana OS i konfiguracija (registry, ini fajle, organizacija registry strukture, keys)
- promjena HW platforme (intel, alpha, powerpc, arm)
- promjena tipa file systema (FATxx, NFTS)
- drugačiji artefakti i formati (recycle bin, print spooler, backup, index, mail, vss, browser)

UNIX

serverski OS i vrlo rijetko korisnički



Linux – kao derivat UNIXa

Distribucije Linuxa – nevjerojatan broj i znatne razlike

- Primjene OS po raznim kriterijima – razne karakteristike koje treba poznavati
- Po OS kriteriju
 - Serverski OS
 - Korisnički OS
- Po kriteriju uređaja
 - Mobilni uređaji
 - Sve moguće HW platforme
 - Embeded uređaji
 - Roboti

Apple Mac

Evolucijska linija poput windowsa

os 1 os 10.x

Raznoliki HW

računala, serveri

mobilni uređaji

dominanto mobilni uređaji danas

OS razni derivati i verzije

razlike u organizaciji i tipu FSa

File systems

FAT, NTFS, EXT, UFS, HSFS .. oko 100 i bez FSa (baze podataka raw partitions)

Razni aspekti koji se mijenjaju:

- Organizacija prostora
- Podržani mediji
- Podržani OS
- prava i vlasništvo nad objektima
- Enkripcija
- Kompresija
- Backup
- Brisanje
- Terminologija

Mobilni uređaji

Svi uređaji u osnovi selfcontained

U užem smislu smatphones

- apple ios,
- android,
- windows

ali i GPS, tableti, stari mobiteli i još štošta

Razni proizvođači

Razni OSovi

Razni FS i načini pohrane i kodiranja podataka

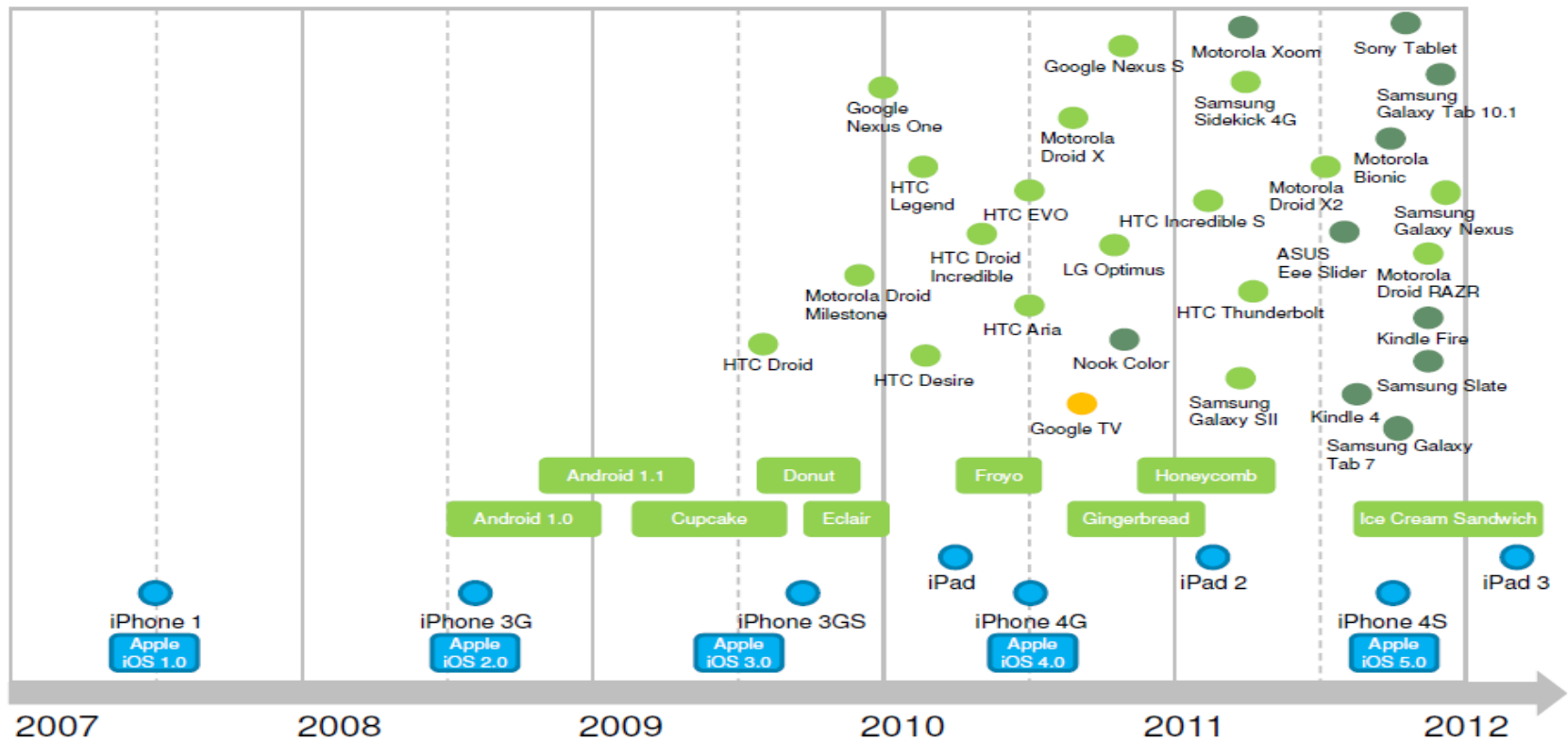
Više izuzetaka nego pravila

Međusobna nekompatibilnost forenzičkih alata

Mobilni OS, platforme i vendori

Platform proliferation

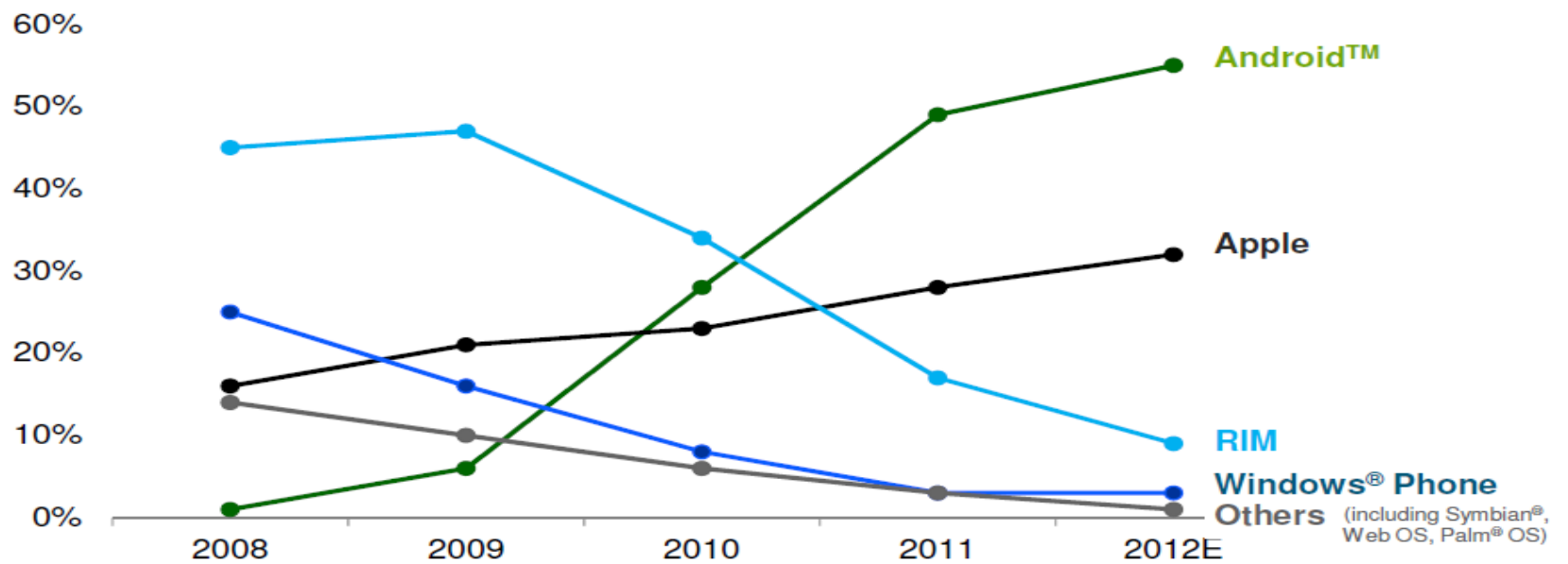
Explosion of OS versions and device flavors



Source: Jeff Haynie / Appcclerator.
 Copyright © 2012 Accenture All rights reserved.

Smartphones - trendovi

Smartphones: A two-horse race with potential for 3rd
 Share of Global Mobile Installed Base of Smartphone OS



Source: Gartner.

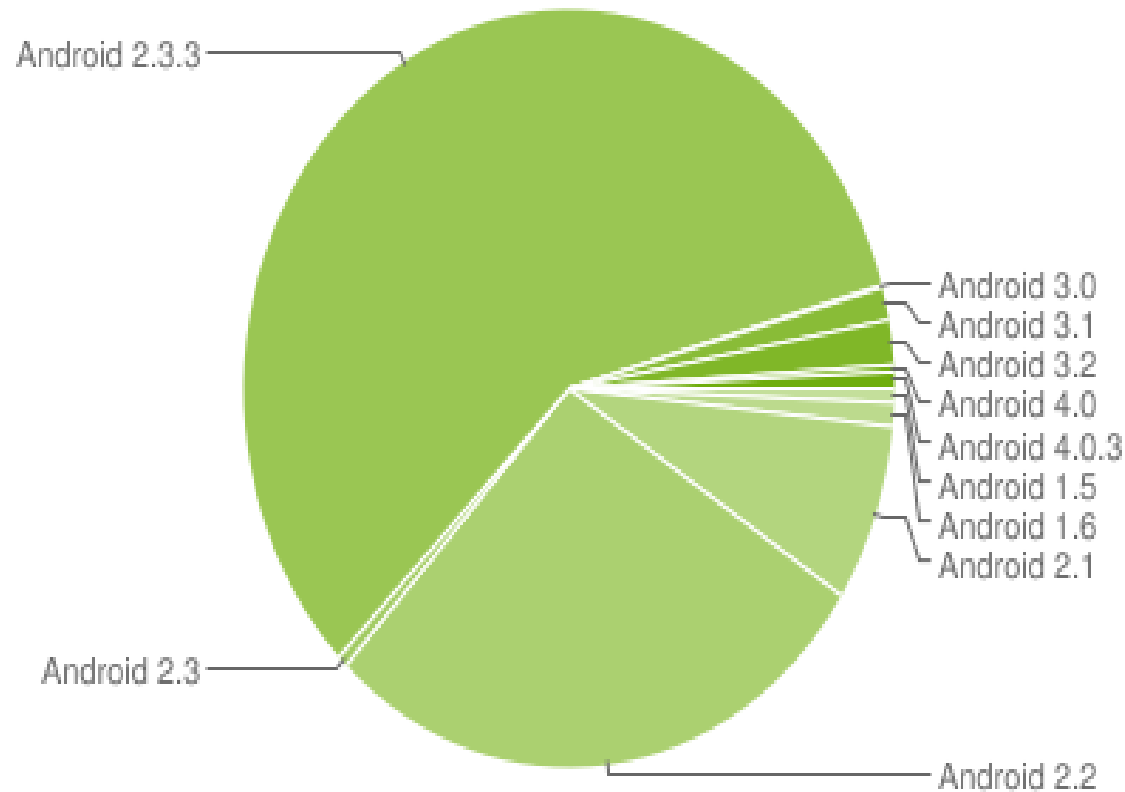
Copyright © 2012 Accenture All rights reserved.

Mobilni uređaji - Android OS

Android najveći očekivani rast

Verzije se međusobno razlikuju a time i artefakti i alati

[Android verzije i svojstva](#)



Mreža i mrežni servisi

Uže područje digitalne forenzike – mrežna forenzika

TCP/IP v4, v6

Legacy mrežni protokoli

Bežične veze posebno područje samo za sebe

Broadband

Malware analiza

Aplikacije i programi

Email klijenti (outlook, webmail)

Email serveri (exchange)

Chat, messengers, voip (skype)

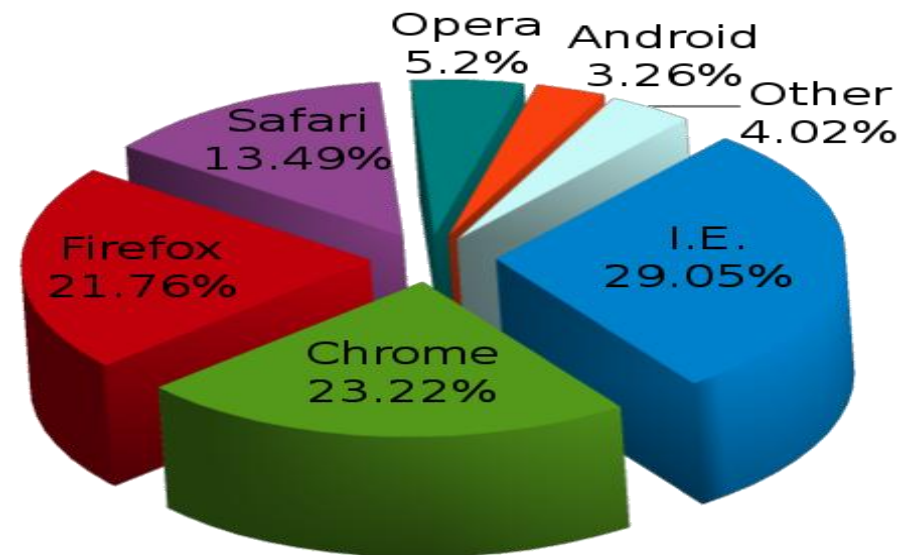
web browseri

explorer

mozilla

opera

chrome



**Browser Usage on Wikimedia
February 2012**

Koji su forenzički relevantni artefakti i gdje ovisno o OS platformi, verziji, konfiguraciji

Kojim alatima se i sa kojom pouzdanošću može doći do artefakata

Linkovi i siteovi

- Internet prepun referenci ...
- Različiti aspekti računalne sigurnosti

<http://forensics.sans.org/community/downloads/>

"SANS Computer forensic and E-Discovery" SANS
portal za računalnu forenziku

Zaključak

- Računalna forenzika je dio kontrole i oporavka od incidenta
 - tu je bitno prepoznavanje (ne)mogućnosti računalne forenzike
- U dogledno vrijeme možemo očekivati sve veću pojavu i objavljivanje incidenata
 - incidenti se ne mogu više držati unutar kuće
 - incidenti moraju biti legalno ispravno odrađeni
- Korištenje metoda računalne forenzike mora biti sustavno i ugrađeno u organizaciju
- Potrebna znanja i postupci moraju biti prepoznati kao nešto što se mora imati na raspolaganju

Bez takvog pristupa sustavi su izuzetno ugroženi

Pitanja ?

damir.delija@insig2.hr

www.insig2.hr