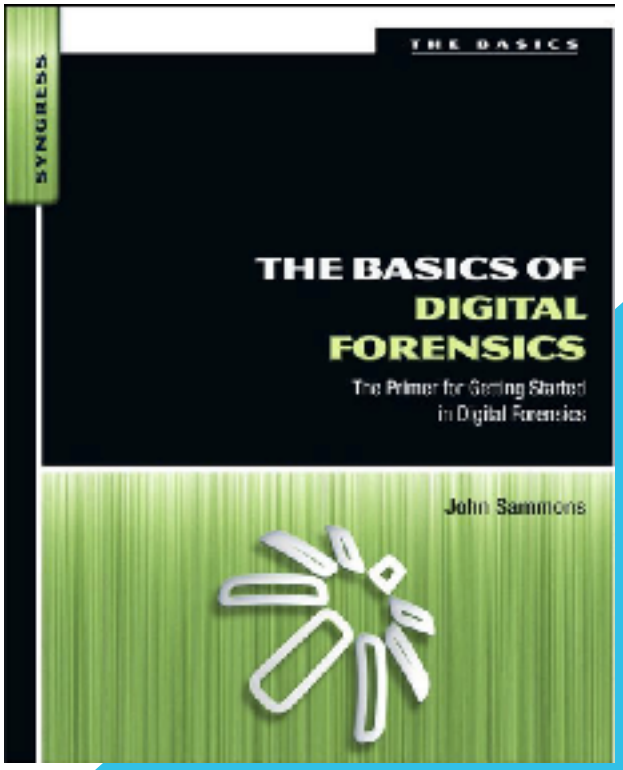


8. INTERNET AND E-MAIL

TOPIK

- Internet
- Web browsers dan evidence yang dihasilkan
- E-mail function dan forensics
- Chat dan social networking evidence

INTERNET OVERVIEW

KONSEP INTERNET

- URL (Uniform Resource Locator)
  - http://www.ccsf.edu/NEW/en/myccsf.html
  - **Protocol:** http
  - **Host:** www
  - **Domain name:** ccsf.edu
  - **Top-level domain:** .edu
  - **Fully qualified domain name:** www.ccsf.edu
  - **Path to file:** NEW/en/myccsf.html
- Browser
  - IE, Chrome, Firefox, Safari, dll.

HTTP PROCESS

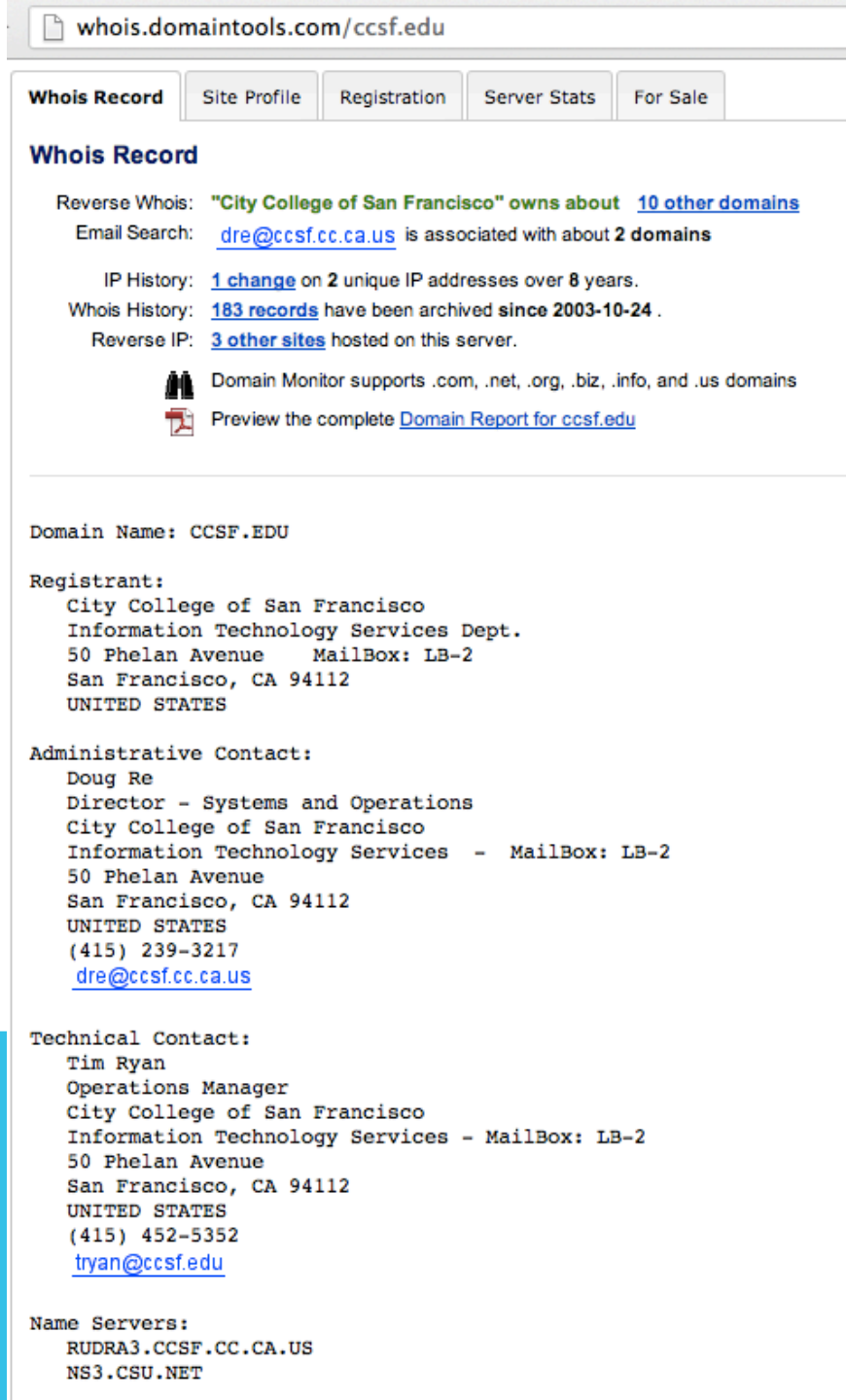
- HTTP (Hypertext Transfer Protocol)
  - Dirancang untuk mengirimkan halaman Web
- Pertama nama domain harus dikonversi ke alamat IP dengan query ke DNS Server (Domain Name Service)
- Maka halaman ini diambil dengan mengirimkan HTTP GET request ke server Web
- Halaman ditulis dalam bentuk HTML (HyperText Markup Language)
  - bisa berisi gambar, video, suara, dll

STATIC DAN DYNAMIC WEB PAGES

- Halaman statis sama untuk setiap pengunjung
- Halaman dinamis dibangun disesuaikan dengan setiap viewer (Web 2.0)
  - Contoh: Facebook, Gmail
  - Mengambil items dari databases
  - **Content Management System** membuat halaman untuk setiap viewer
  - Viewers diidentifikasi oleh **cookies**
- Beberapa kode berjalan pada sisi server, (seperti SQL dan CGI script), dan kode lainnya berjalan pada sisi klien (seperti JavaScript)

WHOIS

- Mengidentifikasi pemilik dari nama domain atau alamat IP yang terdaftar

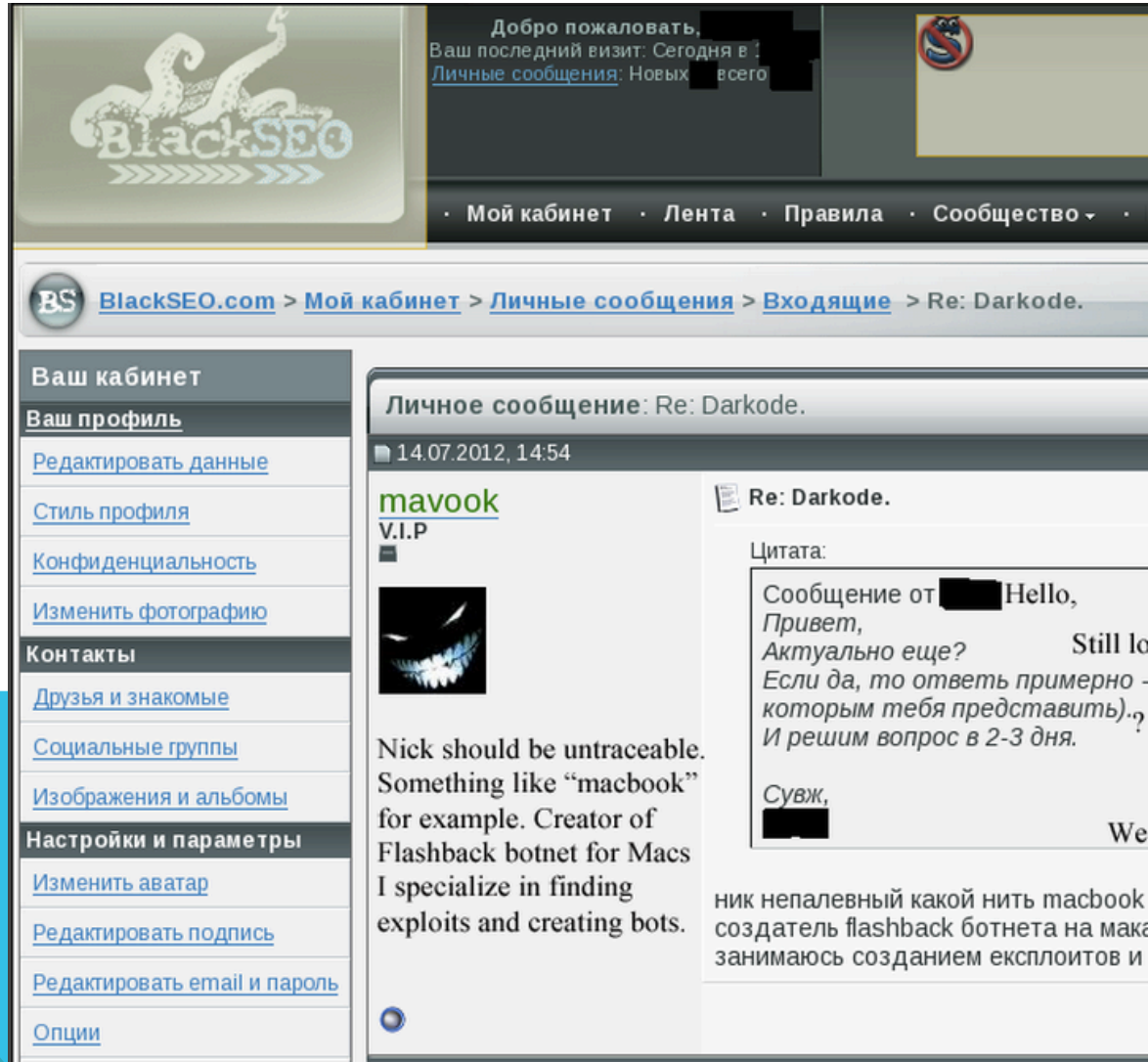


SIAPA YANG MEMBUAT WORM FLASHBACK OS X?

- mavook "mengambil kredit pada" BlackSEO "forum (dalam bahasa Rusia)
- Halaman home pagenya mavook.com tahun 2005

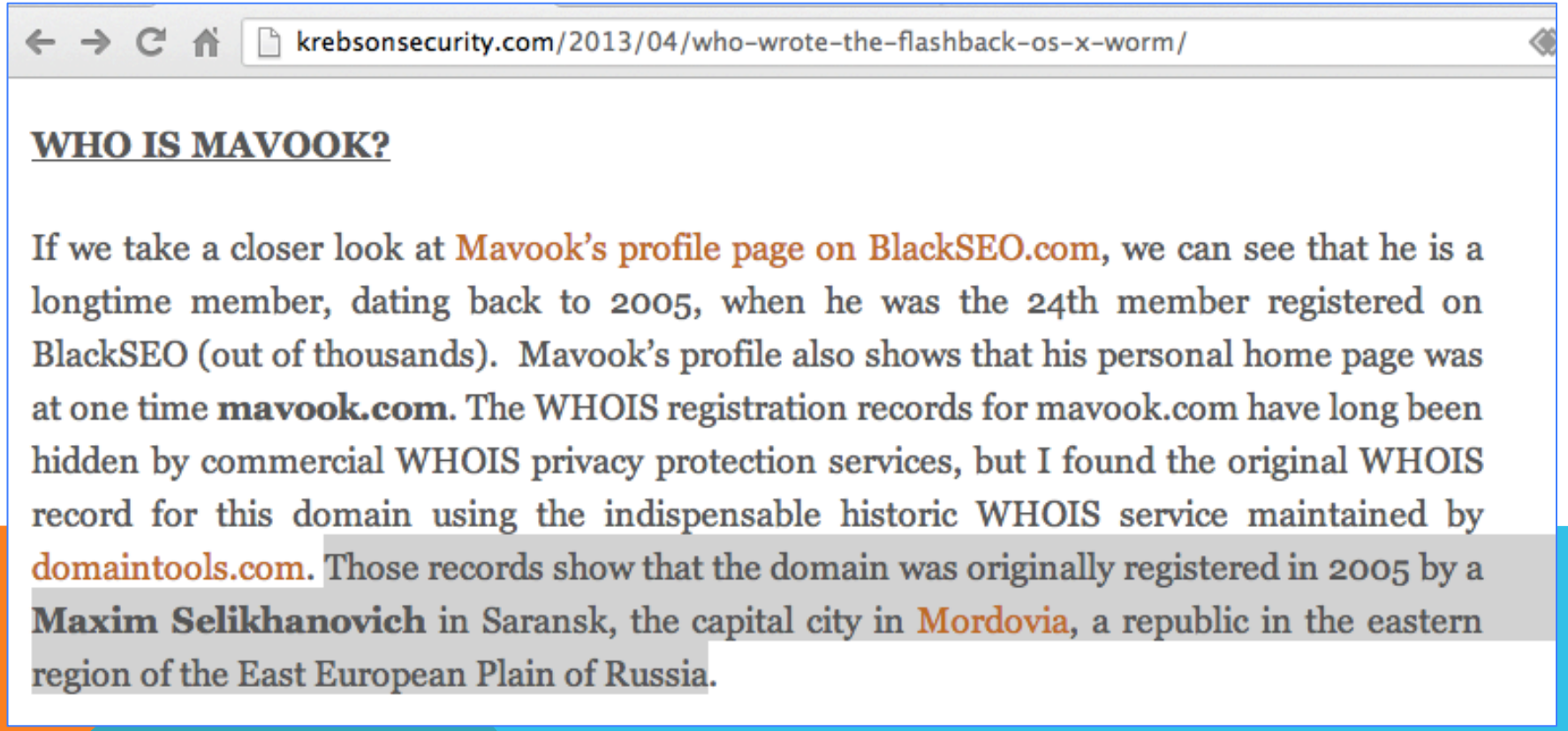
Link

Ch 8a: Who Wrote the Flashback OS X Worm?



WHOIS HISTORY

WHO IS MAVOOK?

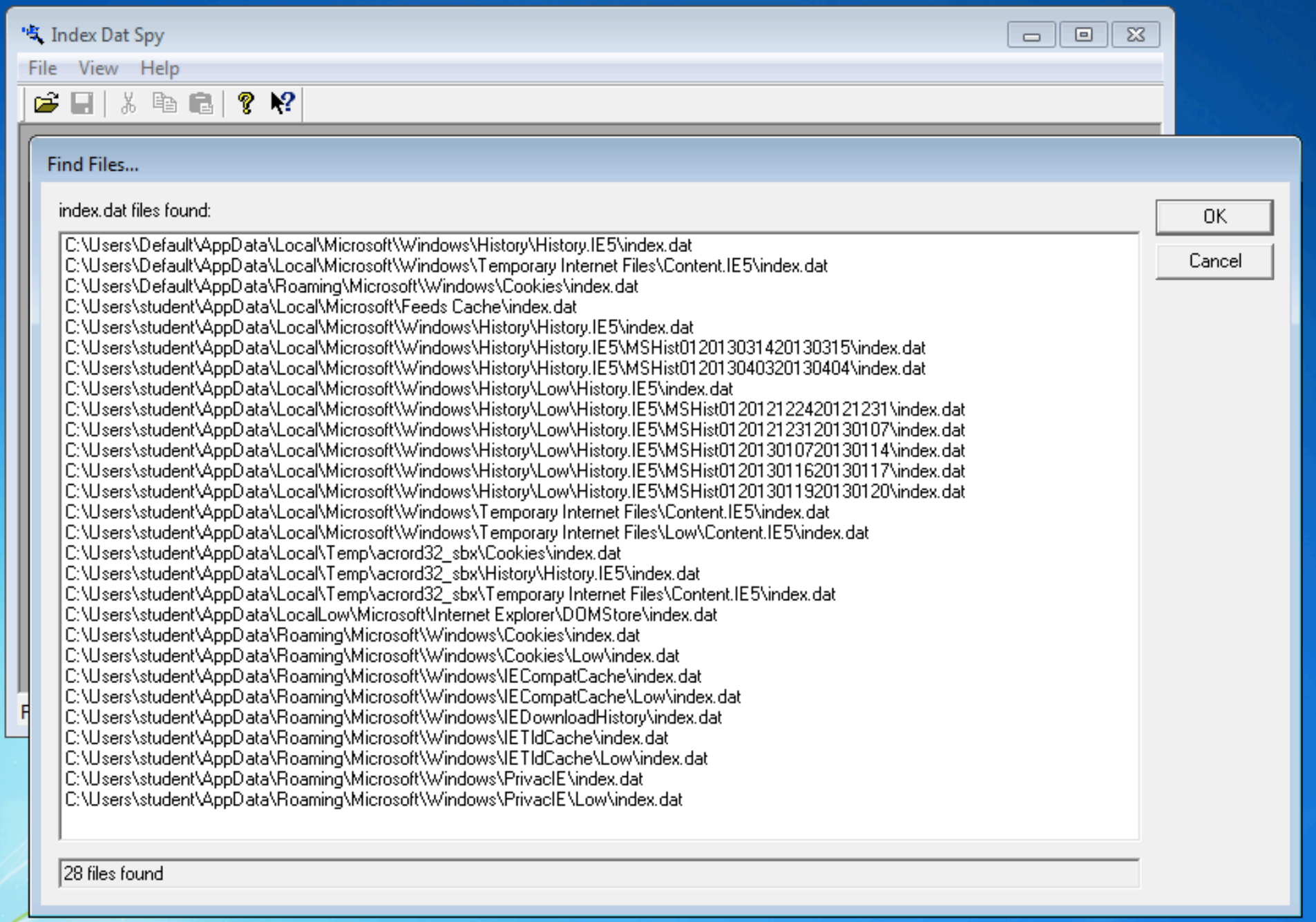


PEER-TO-PEER (P2P)

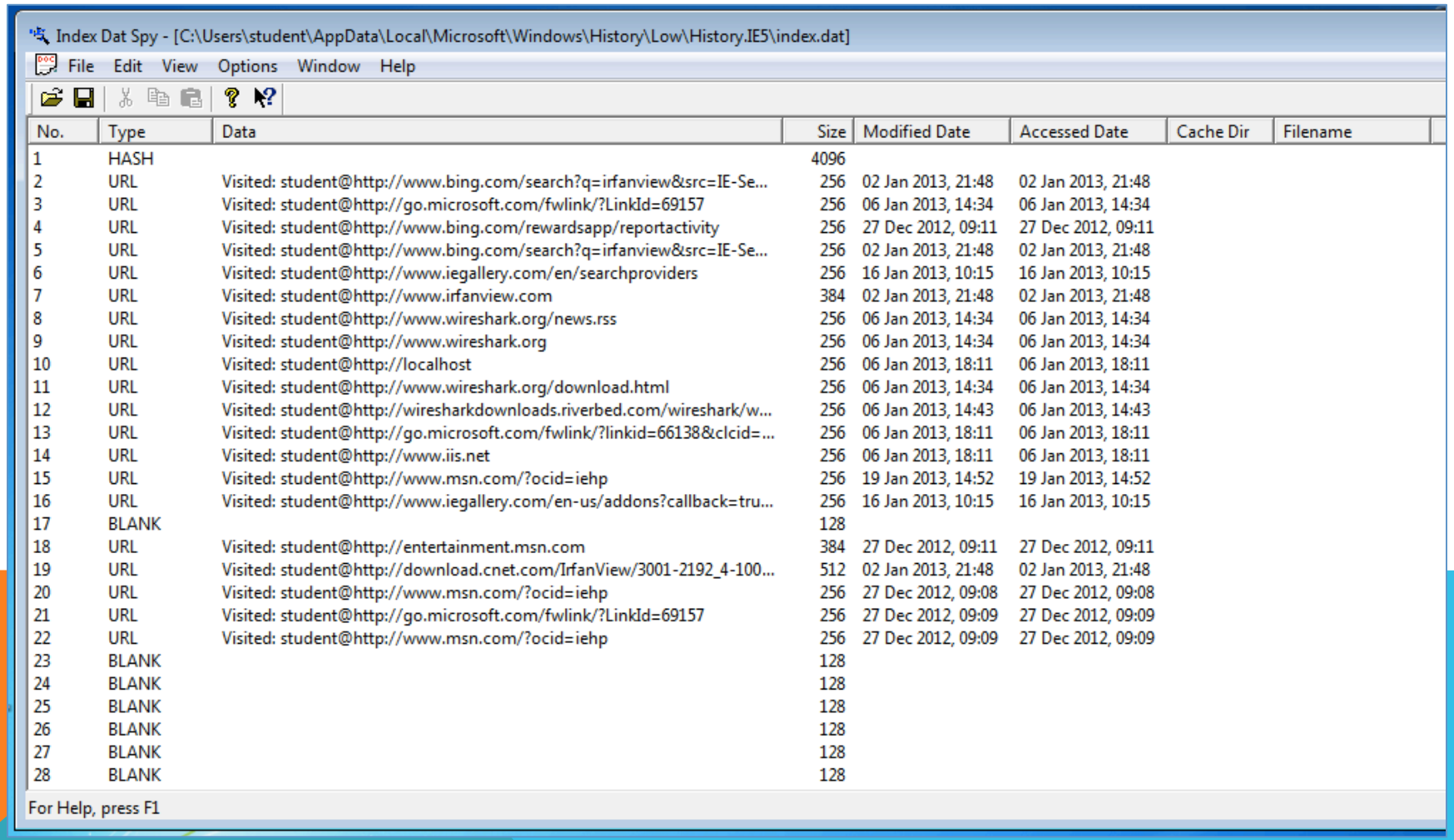
- File-sharing
- Menggunakan protokol Bittorrent
- Sebagian besar lalu lintas P2P digunakan untuk mencuri musik, video, dan perangkat lunak dan konten ilegal lainnya
- Menggunakan sejumlah besar bandwidth dan port
- Contoh: Gnutella, Limewire, uTorrent, Vuze, The Pirate Bay (Link Ch 8b: Gnutella - Wikipedia)

INDEX.DAT FILES

- Binary file yang digunakan oleh Internet Explorer
- Bisa menelusuri URL yang dikunjungi, jumlah kunjungan, dll.
- Link Ch 8c: Where are Index.dat files located? leads to "Index Dat Spy"
  - Paling baik untuk mencari files dan daftarnya
- Link Ch 8d: Index.dat Reader for Windows 7 Vista leads to "Index Dat Reader"
  - Memperlihatkan semua hasil

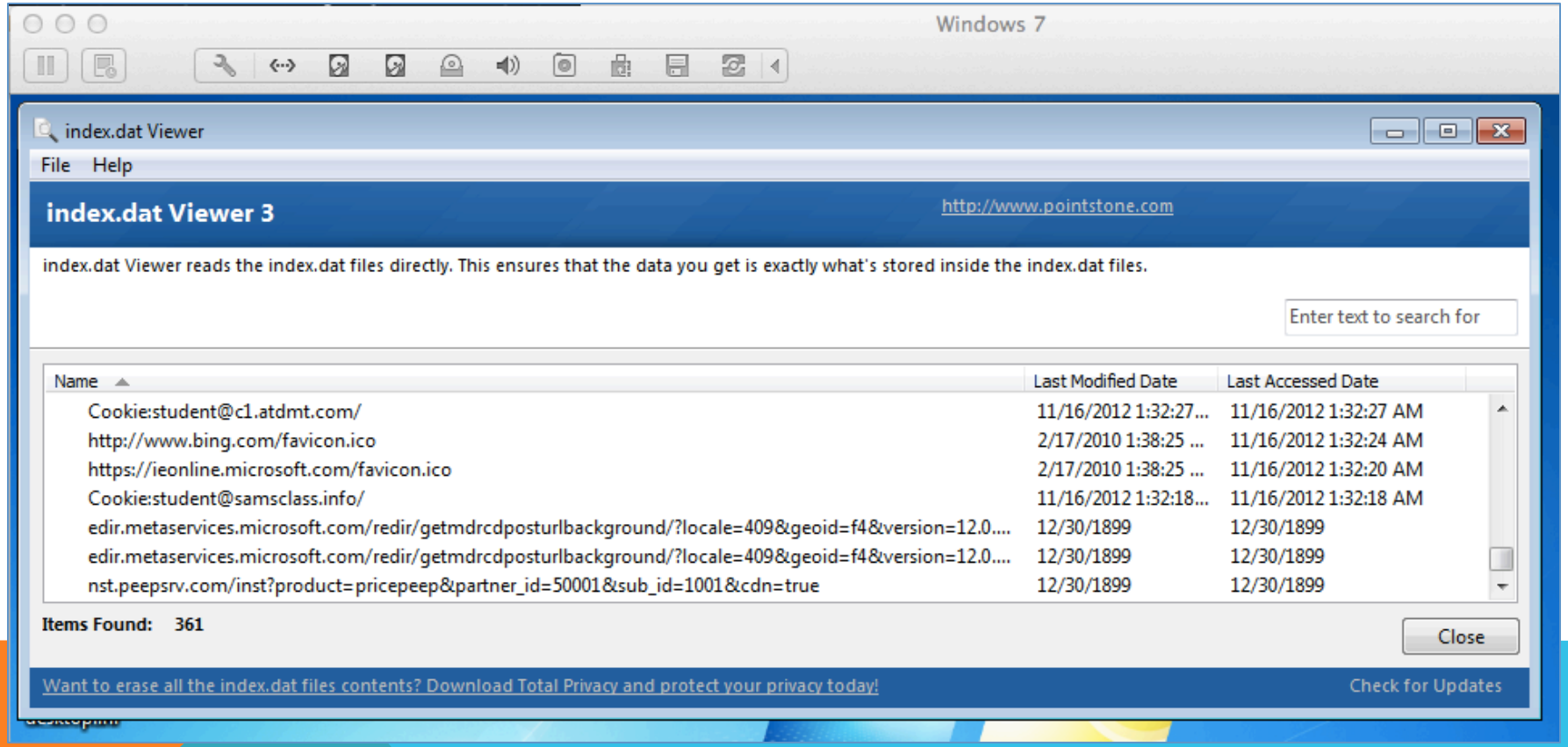

Index Dat Spy
File View Help
Find Files...
index.dat files found:
C:\Users\Default\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Users\Default\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\student\AppData\Local\Microsoft\Feeds Cache\index.dat
C:\Users\student\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Users\student\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012013031420130315\index.dat
C:\Users\student\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012013040320130404\index.dat
C:\Users\student\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat
C:\Users\student\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012012122420121231\index.dat
C:\Users\student\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012012123120130107\index.dat
C:\Users\student\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012013010720130114\index.dat
C:\Users\student\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012013011620130117\index.dat
C:\Users\student\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012013011920130120\index.dat
C:\Users\student\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\student\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\index.dat
C:\Users\student\AppData\Local\Temp\acrord32_sbx\Cookies\index.dat
C:\Users\student\AppData\Local\Temp\acrord32_sbx\History\History.IE5\index.dat
C:\Users\student\AppData\Local\Temp\acrord32_sbx\Temporary Internet Files\Content.IE5\index.dat
C:\Users\student\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\index.dat
C:\Users\student\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\student\AppData\Roaming\Microsoft\Windows\Cookies\Low\index.dat
C:\Users\student\AppData\Roaming\Microsoft\Windows\IECompatCache\index.dat
C:\Users\student\AppData\Roaming\Microsoft\Windows\IECompatCache\Low\index.dat
C:\Users\student\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\index.dat
C:\Users\student\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat
C:\Users\student\AppData\Roaming\Microsoft\Windows\IETldCache\Low\index.dat
C:\Users\student\AppData\Roaming\Microsoft\Windows\PrivacIE\index.dat
C:\Users\student\AppData\Roaming\Microsoft\Windows\PrivacIE\Low\index.dat
OK
Cancel
28 files found

FILES BACK TO 2012!



No.	Type	Data	Size	Modified Date	Accessed Date	Cache Dir	Filename
1	HASH		4096				
2	URL	Visited: student@http://www.bing.com/search?q=irfanview&src=IE-Se...	256	02 Jan 2013, 21:48	02 Jan 2013, 21:48		
3	URL	Visited: student@http://go.microsoft.com/fwlink/?LinkId=69157	256	06 Jan 2013, 14:34	06 Jan 2013, 14:34		
4	URL	Visited: student@http://www.bing.com/rewardsapp/reportactivity	256	27 Dec 2012, 09:11	27 Dec 2012, 09:11		
5	URL	Visited: student@http://www.bing.com/search?q=irfanview&src=IE-Se...	256	02 Jan 2013, 21:48	02 Jan 2013, 21:48		
6	URL	Visited: student@http://www.iegallery.com/en/searchproviders	256	16 Jan 2013, 10:15	16 Jan 2013, 10:15		
7	URL	Visited: student@http://www.irfanview.com	384	02 Jan 2013, 21:48	02 Jan 2013, 21:48		
8	URL	Visited: student@http://www.wireshark.org/news.rss	256	06 Jan 2013, 14:34	06 Jan 2013, 14:34		
9	URL	Visited: student@http://www.wireshark.org	256	06 Jan 2013, 14:34	06 Jan 2013, 14:34		
10	URL	Visited: student@http://localhost	256	06 Jan 2013, 18:11	06 Jan 2013, 18:11		
11	URL	Visited: student@http://www.wireshark.org/download.html	256	06 Jan 2013, 14:34	06 Jan 2013, 14:34		
12	URL	Visited: student@http://wiresharkdownloads.riverbed.com/wireshark/w...	256	06 Jan 2013, 14:43	06 Jan 2013, 14:43		
13	URL	Visited: student@http://go.microsoft.com/fwlink/?linkid=66138&clcid=...	256	06 Jan 2013, 18:11	06 Jan 2013, 18:11		
14	URL	Visited: student@http://www.iis.net	256	06 Jan 2013, 18:11	06 Jan 2013, 18:11		
15	URL	Visited: student@http://www.msn.com/?ocid=iehp	256	19 Jan 2013, 14:52	19 Jan 2013, 14:52		
16	URL	Visited: student@http://www.iegallery.com/en-us/addons?callback=tru...	256	16 Jan 2013, 10:15	16 Jan 2013, 10:15		
17	BLANK		128				
18	URL	Visited: student@http://entertainment.msn.com	384	27 Dec 2012, 09:11	27 Dec 2012, 09:11		
19	URL	Visited: student@http://download.cnet.com/IrfanView/3001-2192_4-100...	512	02 Jan 2013, 21:48	02 Jan 2013, 21:48		
20	URL	Visited: student@http://www.msn.com/?ocid=iehp	256	27 Dec 2012, 09:08	27 Dec 2012, 09:08		
21	URL	Visited: student@http://go.microsoft.com/fwlink/?LinkId=69157	256	27 Dec 2012, 09:09	27 Dec 2012, 09:09		
22	URL	Visited: student@http://www.msn.com/?ocid=iehp	256	27 Dec 2012, 09:09	27 Dec 2012, 09:09		
23	BLANK		128				
24	BLANK		128				
25	BLANK		128				
26	BLANK		128				
27	BLANK		128				
28	BLANK		128				

INDEX.DAT READER SHOWS ALL ENTRIES



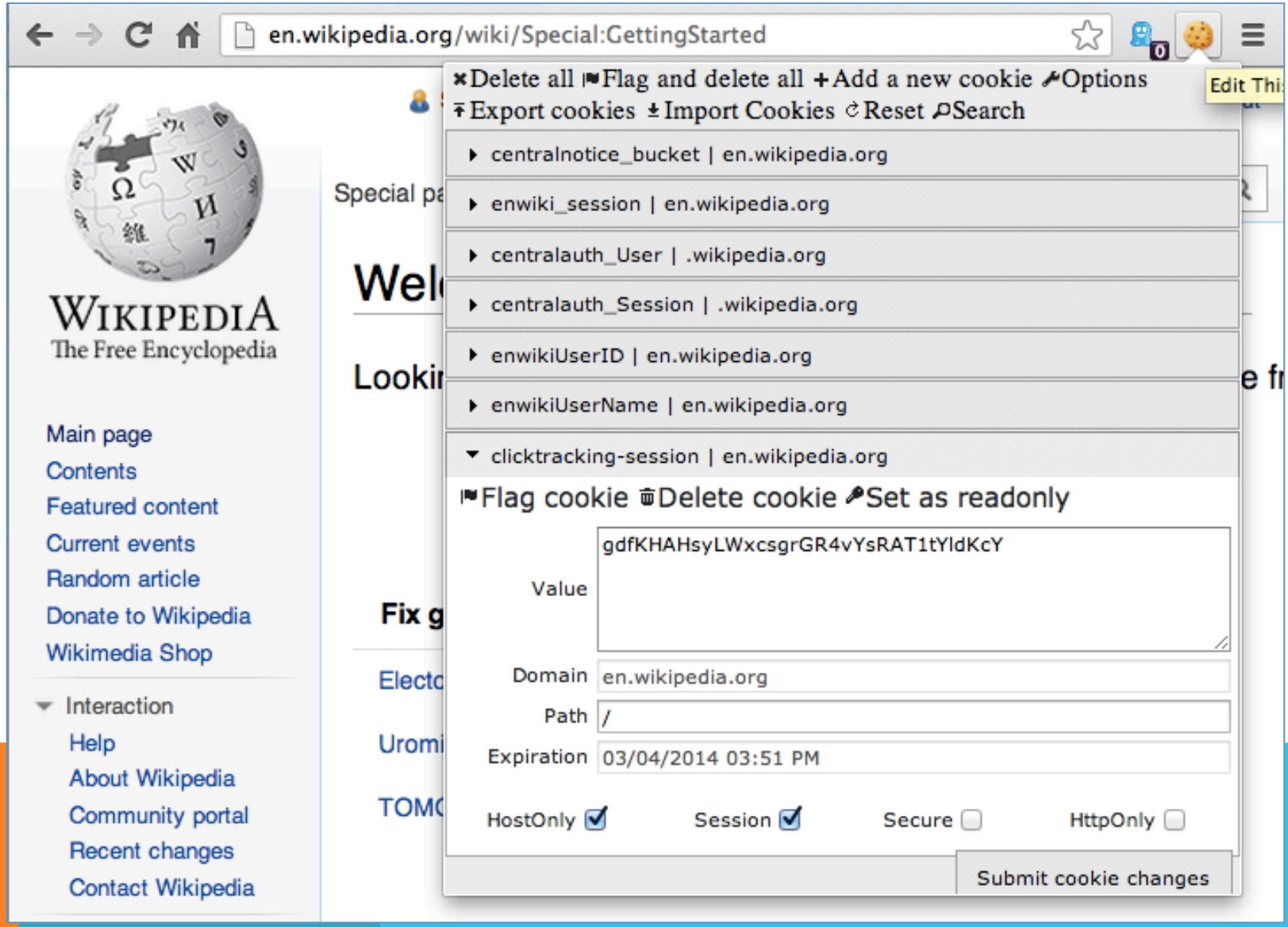
Back TO 1899!

- (INGAT jangan percaya pada tools!)

WEB BROWSERS

COOKIES

"Edit This Cookie" Chrome Extension (Link Ch 8e: Ghostery)


en.wikipedia.org/wiki/Special:GettingStarted
Delete all
Flag and delete all
Add a new cookie
Options
Export cookies
Import Cookies
Reset
Search
centralnotice_bucket | en.wikipedia.org
enwiki_session | en.wikipedia.org
centralauth_User | .wikipedia.org
centralauth_Session | .wikipedia.org
enwikiUserID | en.wikipedia.org
enwikiUserName | en.wikipedia.org
clicktracking-session | en.wikipedia.org
Flag cookie
Delete cookie
Set as readonly
Value
gdfKHAHsyLWxcsgrGR4vYsRAT1tYldKcY
Domain
en.wikipedia.org
Path
/
Expiration
03/04/2014 03:51 PM
HostOnly
Session
Secure
HttpOnly
Submit cookie changes
WIKIPEDIA
The Free Encyclopedia
Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikimedia Shop
Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact Wikipedia

COOKIES

- File Plain text
- Sering disadap oleh pihak ketiga
- Sebuah cookie dari situs TIDAK membuktikan pengguna mengunjungi situs tersebut

www.ghostery.com

Ghostery™

DOWNLOAD NOW

ABOUT G

Detect

Ghostery™ sees the invisible web - tags, web bugs, pixels and beacons. Ghostery tracks the trackers and gives you a roll-call of the ad networks, behavioral data providers, web publishers, and other companies interested in your activity.

www.sfgate.com

SUMMER OF

JULY 4TH - SEPTE

San Francisco Chronicle

Subscribe now and save over 50%

SFGate

Wednesday Apr 03, 2013 3:36 PM PT

Home | News | Sports | Business | Entertain

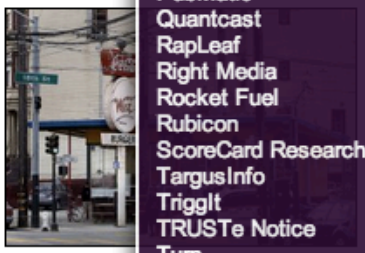
Don't Miss: Ebert's cancer returns | SF's new mozz

TODAY IN SPORTS

Cal junior Allen

Rare birds' nest destroyed

Federal probe is triggered after home of rare raptors atop S.F. crane is smashed to bits.



S.F.'s 25 'le

This burger j list of 'heritage' places. It's not the only surprise. See the whole list.

Wright hor

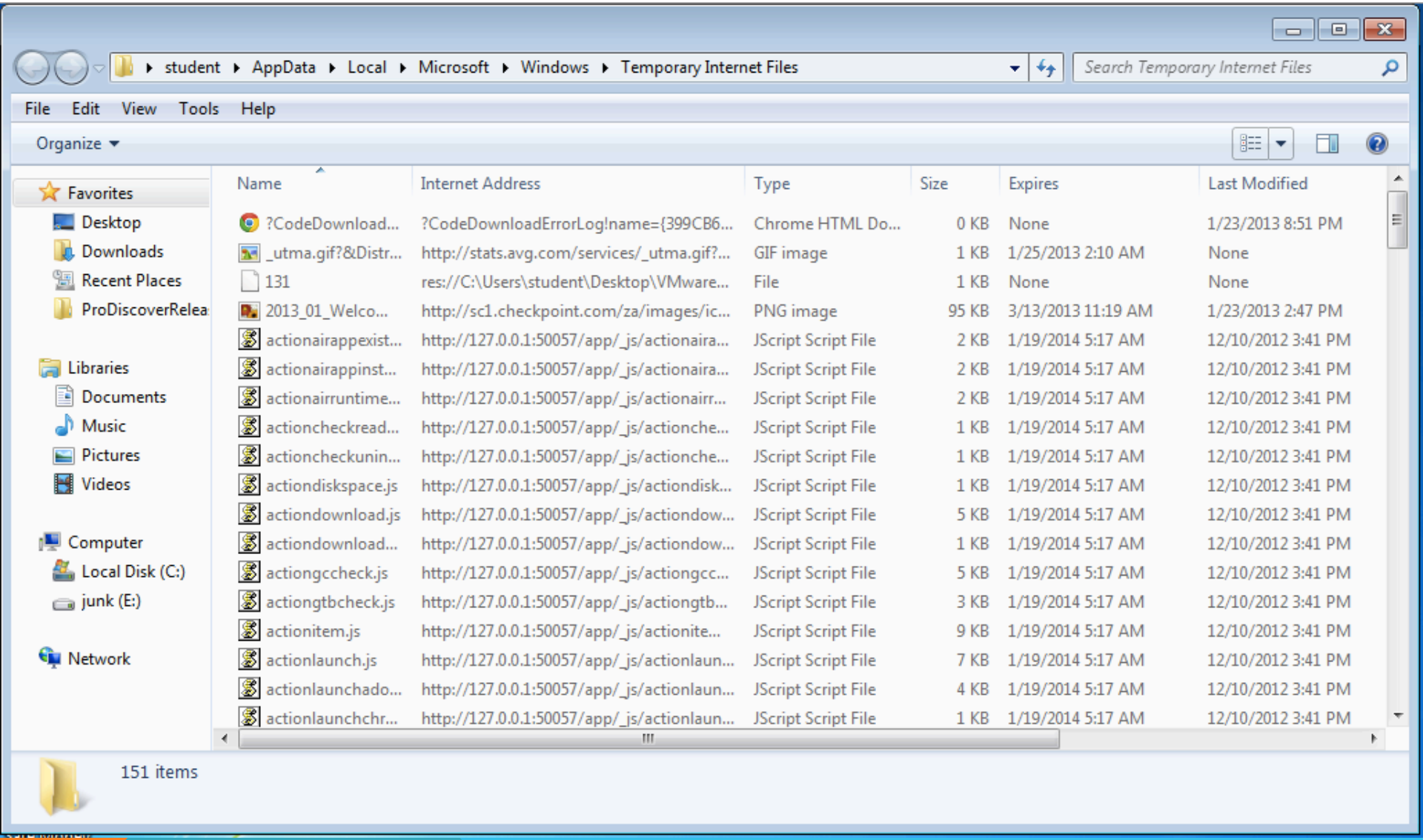
Two Bay Are architect are getting little

- 24/7 Media
- Acerno
- Adap.tv
- AdMeld
- Aggregate Knowledge
- AlmondNet
- AMP Platform
- AppNexus
- Auditude
- CoreAudience
- Demdex
- DoubleClick
- eXelate
- Genome
- Google +1
- Google Adsense
- Google Analytics
- iCrossing
- JumpTime
- Legolas Media
- Lotame
- Meebo Bar
- Microsoft Atlas
- NetRatings SiteCensus
- News Registry
- Omniture
- OpenX
- PubMatic
- Quantcast
- RapLeaf
- Right Media
- Rocket Fuel
- Rubicon
- ScoreCard Research Beacon
- TargusInfo
- Triggit
- TRUSTe Notice
- Turn
- Yahoo! Overture

TEMPORARY INTERNET FILES

- atau Web Cache
- Membuat halaman di reload lebih cepat
  - Internet Options, General tab, di bawah Browsing history, click Settings. In the Settings dialog box, Pada kotak dialog Pengaturan, klik Lihat file.

- Link : Melihat cache (Temporary file) pada IE, Firefox dan Opera


student ▸ AppData ▸ Local ▸ Microsoft ▸ Windows ▸ Temporary Internet Files
Search Temporary Internet Files
File Edit View Tools Help
Organize
Favorites
Desktop
Downloads
Recent Places
ProDiscoverRelea
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
junk (E:)
Network
Name | Internet Address | Type | Size | Expires | Last Modified
?CodeDownload... | ?CodeDownloadErrorLog!name={399CB6... | Chrome HTML Do... | 0 KB | None | 1/23/2013 8:51 PM
_utma.gif?&Distr... | http://stats.avg.com/services/_utma.gif?... | GIF image | 1 KB | 1/25/2013 2:10 AM | None
131 | res://C:\Users\student\Desktop\VMware... | File | 1 KB | None | None
2013_01_Welco... | http://sc1.checkpoint.com/za/images/ic... | PNG image | 95 KB | 3/13/2013 11:19 AM | 1/23/2013 2:47 PM
actionairappexist... | http://127.0.0.1:50057/app/_js/actionaira... | JScript Script File | 2 KB | 1/19/2014 5:17 AM | 12/10/2012 3:41 PM
actionairappinst... | http://127.0.0.1:50057/app/_js/actionaira... | JScript Script File | 2 KB | 1/19/2014 5:17 AM | 12/10/2012 3:41 PM
actionairruntime... | http://127.0.0.1:50057/app/_js/actionairr... | JScript Script File | 2 KB | 1/19/2014 5:17 AM | 12/10/2012 3:41 PM
actioncheckread... | http://127.0.0.1:50057/app/_js/actionche... | JScript Script File | 1 KB | 1/19/2014 5:17 AM | 12/10/2012 3:41 PM
actioncheckunin... | http://127.0.0.1:50057/app/_js/actionche... | JScript Script File | 1 KB | 1/19/2014 5:17 AM | 12/10/2012 3:41 PM
actiondiskspace.js | http://127.0.0.1:50057/app/_js/actiondisk... | JScript Script File | 1 KB | 1/19/2014 5:17 AM | 12/10/2012 3:41 PM
actiondownload.js | http://127.0.0.1:50057/app/_js/actiondow... | JScript Script File | 5 KB | 1/19/2014 5:17 AM | 12/10/2012 3:41 PM
actiondownload... | http://127.0.0.1:50057/app/_js/actiondow... | JScript Script File | 1 KB | 1/19/2014 5:17 AM | 12/10/2012 3:41 PM
actiongccheck.js | http://127.0.0.1:50057/app/_js/actiongcc... | JScript Script File | 5 KB | 1/19/2014 5:17 AM | 12/10/2012 3:41 PM
actiongtbcheck.js | http://127.0.0.1:50057/app/_js/actiongtb... | JScript Script File | 3 KB | 1/19/2014 5:17 AM | 12/10/2012 3:41 PM
actionitem.js | http://127.0.0.1:50057/app/_js/actionite... | JScript Script File | 9 KB | 1/19/2014 5:17 AM | 12/10/2012 3:41 PM
actionlaunch.js | http://127.0.0.1:50057/app/_js/actionlaun... | JScript Script File | 7 KB | 1/19/2014 5:17 AM | 12/10/2012 3:41 PM
actionlaunchado... | http://127.0.0.1:50057/app/_js/actionlaun... | JScript Script File | 4 KB | 1/19/2014 5:17 AM | 12/10/2012 3:41 PM
actionlaunchchr... | http://127.0.0.1:50057/app/_js/actionlaun... | JScript Script File | 1 KB | 1/19/2014 5:17 AM | 12/10/2012 3:41 PM
151 items

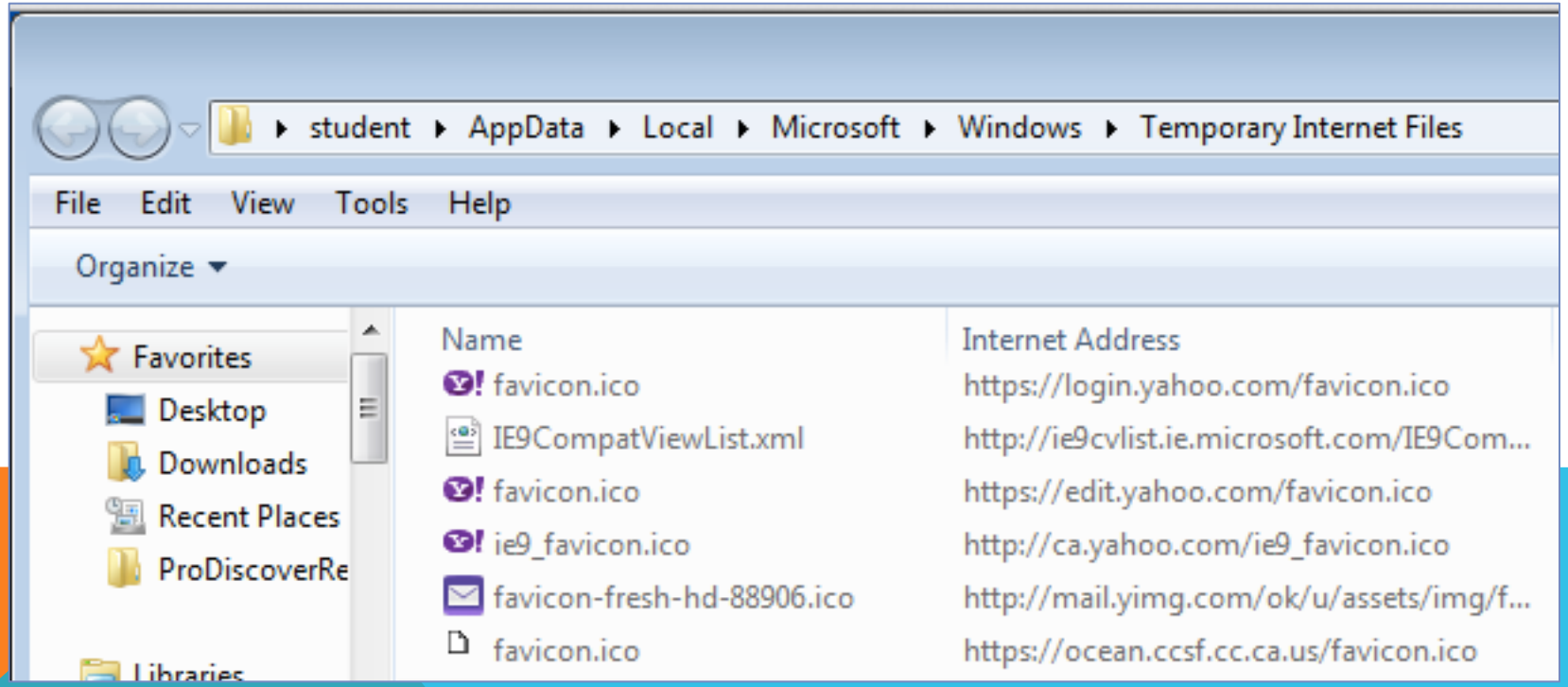
ERROR IN TEXTBOOK

HTTPS resources dicached oleh Internet Explorer sama seperti HTTP resources

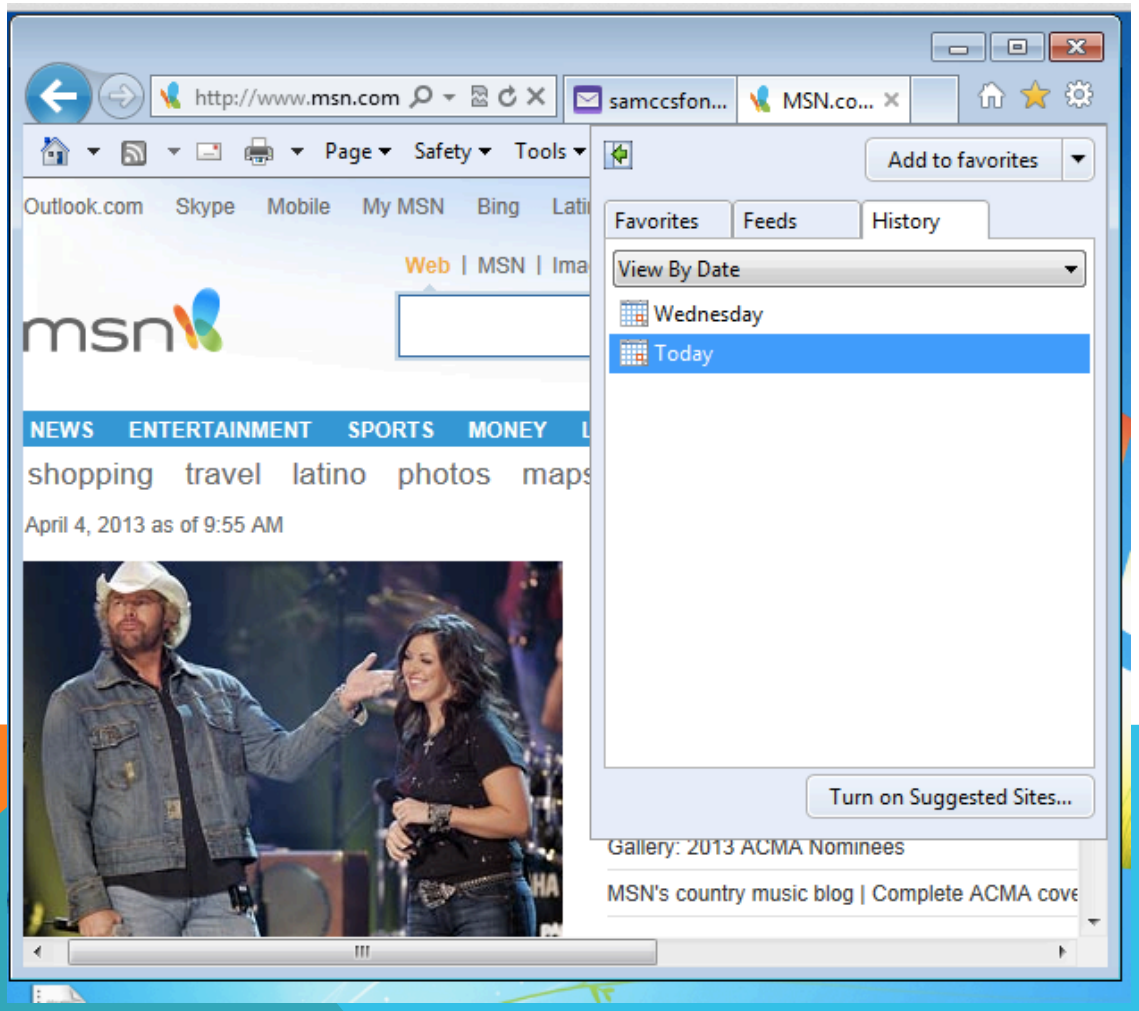
Link:

ERROR IN TEXTBOOK

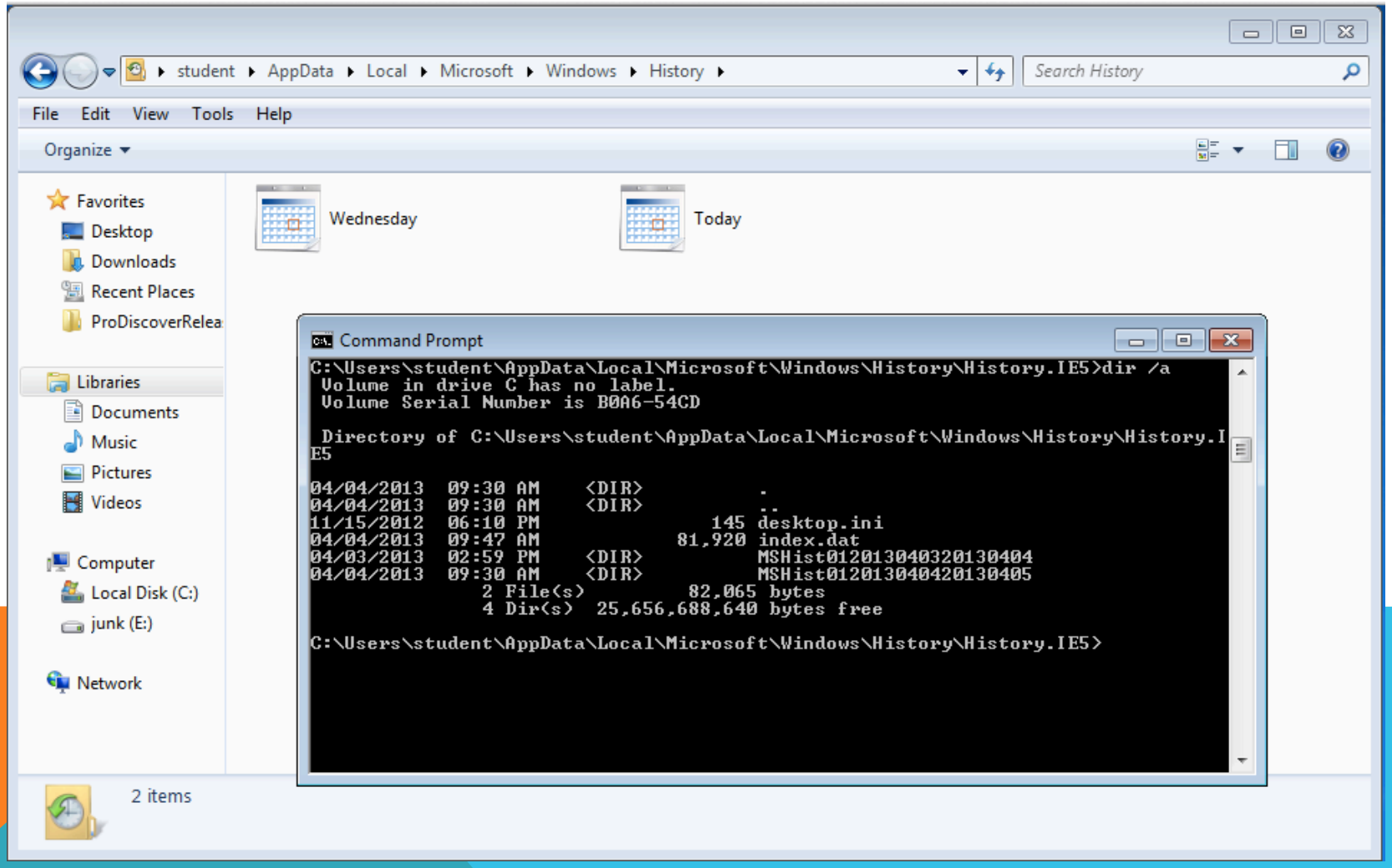
HTTPS Caching and Internet Explorer



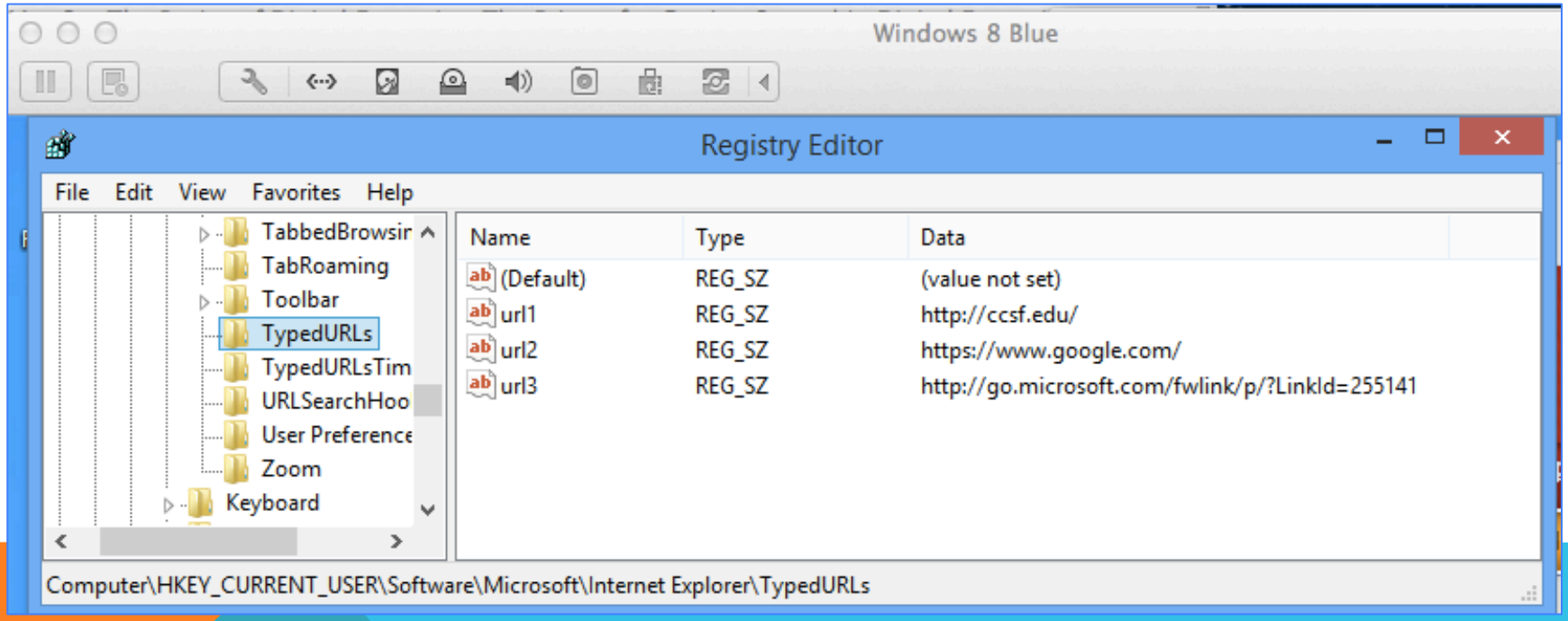
INTERNET HISTORY



INTERNET HISTORY



TYPEDURLS


Windows 8 Blue
Registry Editor
File Edit View Favorites Help
TabbedBrowsir
TabRoaming
Toolbar
TypedURLs
TypedURLsTim
URLSearchHoo
User Preference
Zoom
Keyboard
Name Type Data
(Default) REG_SZ (value not set)
url1 REG_SZ http://ccsf.edu/
url2 REG_SZ https://www.google.com/
url3 REG_SZ http://go.microsoft.com/fwlink/p/?LinkId=255141
Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

CHAT CLIENTS

CHAT CLIENTS POPULER

- AOL Instant Messenger
- Yahoo! Messenger
- Windows Live Messenger
- Trillian
- ICQ
- Banyak lagi
- Popular di antara pedophiles

Yahoo shuts chat rooms promoting adult-child sex

October 12, 2005

> Some rooms carried labels such as "kiddies who love sex," "girls 13 & up for much older men," "8-12 yo girls for older men" and "teen girls for older fat men." Many were located in chat categories titled "Schools and Education" and "Teen."

Link Ch 8h: Yahoo shuts chat rooms promoting adult-child sex (from 2005)

DATA DARI CHAT CLIENTS

- Contact atau “Buddy” list
- Block list
- Daftar chats terbaru
- Logging dari chats
- Manually saved chat logs
- Daftar penerimaan untuk video chat, transfer file, pesan pribadi
- Ponsel yang terkait dengan akun

IRC (INTERNET RELAY CHAT)

- No central authority
- IRC Networks

  Undernet, IRCNet, Efnet, etc.

Link Ch 8i: IRC: 99.9 illegal

IRC Analysis - 99.9% Illegal?

Hacker's Playground or Researcher's Dream?

Keyword	Occurrences	Legal Contexts	Illegal Contexts
Norton	4431	4	4427
Microsoft	3227	6	3221
Symantec	2568	0	2568
Jasc	372	0	372

ICQ

- 42 juta pengguna aktif
- Rata-rata pengguna yang terhubung lebih dari 5 jam per hari
- 47% perempuan
- 80% dari pengguna antara 13 dan 29
- High level of privacy – hanya user yang diundang dapat chatting dengan Anda

EMAIL

VALUE OF EMAIL

- Salah satu sumber barang bukti terbaik
- Orang sering lupa bahwa email tidak bersifat pribadi

April 28, 1999 8:50 PM PDT

Microsoft emails focus on DR-DOS threat

Microsoft also debated the exact language the message should contain. In the end, senior vice president Brad Silverberg said in a 1992 email that the message needed to steer users away from DR-DOS. "What the [user] is supposed to do is feel uncomfortable, and when he has bugs, suspect that the problem is DR-DOS and then go out to buy MS-DOS," Silverberg wrote.

The proposed message caused Brad Chase, Microsoft's vice president, to warn that the code detecting DR-DOS "better be perfect. Otherwise you could be in a heap [sic] of trouble."

"If you're going to kill someone there isn't much reason to get all worked up about it and angry," Allchin wrote in an email discussing how Microsoft should compete against Novell. "Any discussions beforehand are a waste of time. We need to smile at Novell while we pull the trigger."

Link Ch 8j: Microsoft emails focus on DR-DOS threat

Oracle counsel quizzes Google's Rubin about Java emails

Summary: *The founder and father of Android, Andy Rubin, was finally called to the stand in the Oracle v. Google trial to testify about licensing discussions regarding Java.*

By Rachel King for Between the Lines | April 23, 2012 -- 13:09 GMT (06:09 PDT)

Follow @rachelking

The first one from Rubin to Lindholm, dated July 29, 2005, included an agenda, which had the bullet point, "Google needs a TCK license."

Furthermore, in another email Rubin wrote in December 2005,

My reasoning is that either a) we'll partner with Sun as contemplated in our most recent discussion or b) we'll take a license. i think a clean room implementation is unlikely because of the teams prior knowledge.

Link CH 8k: Oracle counsel quizzes Google's Rubin about Java emails

Obama: first president to use email?

by LUCY on JANUARY 24, 2009 · LEAVE A COMMENT · in THINK/PRAY

It sounds pretty outrageous, but Obama will be the first sitting president to use email. I don't know about you, but I can not remember life before email and I can not imagine my life now without email. To me, this restriction is symbolic for the larger sacrifice that a president must make: his freedom.

Obama's personal win: Keeping the BlackBerry

Link Ch 8I: Obama: first president to use email?

BAGAIMANA EMAIL DIAKSES

- Web-based mail
  - Gmail atau Hotmail
  - Di akses melalui browser
- Email client
  - Outlook
    - Menyimpan data dalam format file .pst atau .ost
    - Format Proprietary database (Link Ch 8m: Personal Storage Table - Wikipedia)
  - Windows Live Mail (pendahulu Outlook Express)
    - Outlook Express menggunakan file .DBX (databases)
    - Windows Live Mail menggunakan file .EML (plain text files, satu tiap message)

PROTOKOL EMAIL

- SMTP (Simple Mail Transfer Protocol)
  - Digunakan untuk mengirim email dari satu server ke yang lain
- Post Office Protocol (POP)
  - Digunakan oleh klien email untuk menerima pesan email
- Internet Message Access Protocol (IMAP)
  - Digunakan oleh klien email untuk menerima pesan email, memiliki fitur lebih dari POP

EMAIL SEBAGAI EVIDENCE

- Komunikasi yang relevan dengan kasus
- alamat email
- alamat IP
- Tanggal dan waktu

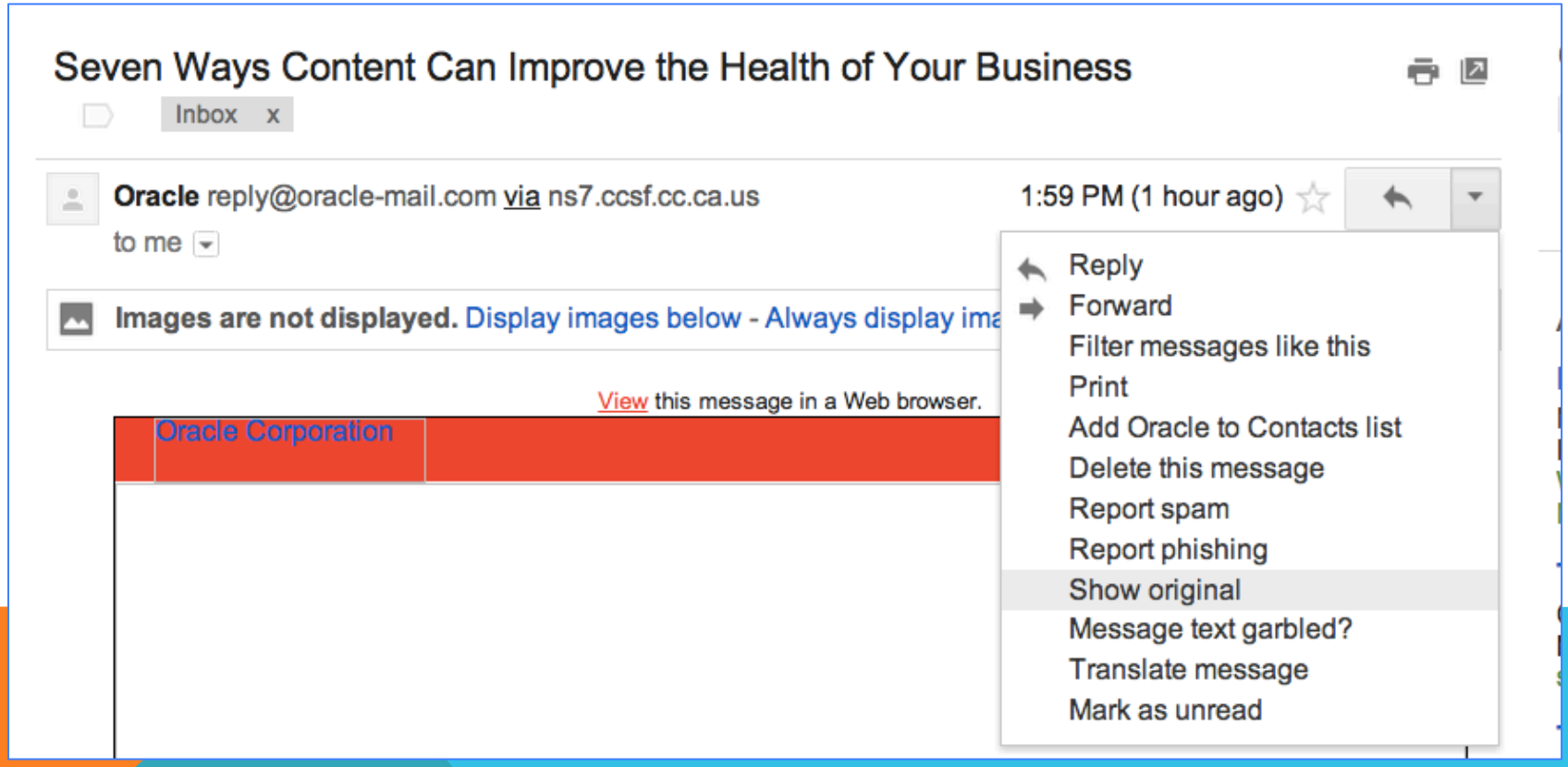
WHERE EMAIL CAN BE FOUND

- Komputer tersangka
- Setiap komputer penerima
- Perusahaan server SMTP
- media backup
- smartphone
- penyedia layanan
- Setiap server email yang dilewati

KOMPONEN EMAIL

- Header
  - Menunjukkan server email yang dilalui
- Body
  - Pesan yang dibaca
  - Attachments (lampiran)

GMAIL: “SHOW ORIGINAL”



HEADER

```
Delivered-To: sam.bowne@gmail.com
Received: by 10.227.94.198 with SMTP id a6csp233034wbn;
        Thu, 4 Apr 2013 14:17:02 -0700 (PDT)
X-Received: by 10.67.4.227 with SMTP id ch3mr5148977pad.59.1365110221339;
        Thu, 04 Apr 2013 14:17:01 -0700 (PDT)
Return-Path: <>
Received: from ns7.ccsf.cc.ca.us (ns7.ccsf.cc.ca.us. [147.144.1.250])
        by mx.google.com with ESMTPS id qp8si12051995pbc.243.2013.04.04.14.17.00
        (version=TLSv1 cipher=RC4-SHA bits=128/128);
        Thu, 04 Apr 2013 14:17:01 -0700 (PDT)
Received-SPF: pass (google.com: best guess record for domain of ns7.ccsf.cc.ca.us designates 147.144.1.250 as permitted sender) client-
ip=147.144.1.250;
Authentication-Results: mx.google.com;
       spf=pass (google.com: best guess record for domain of ns7.ccsf.cc.ca.us designates 147.144.1.250 as permitted sender) smtp.mail=
Received: from bat-gwia.ccsf.edu (bat-gwia.ccsf.edu [10.2.0.231])
        by ns7.ccsf.cc.ca.us (8.13.1/8.13.1) with ESMTP id r34LH0vv014721
        for <sam.bowne@gmail.com>; Thu, 4 Apr 2013 14:17:00 -0700
Received: from GWIA_DOM-MTA by bat-gwia.ccsf.edu
        with Novell_GroupWise; Thu, 04 Apr 2013 14:17:00 -0700
Received: from barracuda.ccsf.edu (barracuda.ccsf.cc.ca.us [147.144.1.30])
        by bat-gwia.ccsf.edu with ESMTP; Thu, 04 Apr 2013 14:16:50 -0700
Received: from ns7.ccsf.cc.ca.us (ns7.ccsf.cc.ca.us [147.144.1.250]) by barracuda.ccsf.edu with ESMTP id EUSqxgzkHbg97DUd for
<sbowne@barracuda.ccsf.cc.ca.us>; Thu, 04 Apr 2013 14:16:49 -0700 (PDT)
Received: from acsinet63.oracleeblast.com (acsinet63.oracleeblast.com [141.146.5.63])
        by ns7.ccsf.cc.ca.us (8.13.1/8.13.1) with ESMTP id r34LGmJs014661
        for <sbowne@ccsf.edu>; Thu, 4 Apr 2013 14:16:49 -0700
Received: from amts748.us.oracle.com (amts748.us.oracle.com [140.84.104.66])
        by acsinet63.oracleeblast.com (8.14.4+Sun/8.14.4) with ESMTP id r34Kvohb027585
        for <sbowne@ccsf.edu>; Thu, 4 Apr 2013 20:59:24 GMT
Date: Thu, 4 Apr 2013 20:59:24 GMT
From: "Oracle" <reply@oracle-mail.com>
To: <sam.bowne@gmail.com>
MIME-Version: 1.0
Sender: "Oracle" <reply@oracle-mail.com>
Subject: Seven Ways Content Can Improve the Health of Your Business
Reply-To: reply@oracle-mail.com
Message-ID: <SEMA-CR-3-3QZLJN3@bounce.oracle-mail.com>
Content-Type: multipart/alternative; boundary=BF_1365108900197_1110382789
X-Virus-Scanned: by bsmtpd at ccsf.edu


--BF_1365108900197_1110382789
Content-Type: text/plain; charset=UTF-8

Webcast Seven Ways Content Can Improve the Health of Your Business.
```

MENUTUPI JEJAK– EMAIL

Spoofing

- Memalsukan asal email

Anonymous Remailer

- Strip header
- Forwards email tanpa header
- Biasanya tidak menyimpan log
- Melindungi privasi pengguna

Contoh Penggunaan:

How to Use an Anonymous Remailer

SHARED EMAIL ACCOUNTS

- Buat akun pada layanan Web gratis seperti Yahoo!
- Bagikan username dan password dengan penerima
- Tuls email jangan dikirim
- Simpan di folder “Drafts”
- Penerima dapat log in dan melihat
- Digunakan oleh teroris
- Bisa “One-Time Account”

MAILINATOR

- Tidak bisa mengirim, hanya menerima
- Tidak ada password atau privasi

To: **sam**

From: **Sam Bowne**
Subject: **DEMO OF MAILINATOR**
Charset: **ISO-8859-1** **(view as UTF-8)**

Delete

Formatted Forward

Experimental View

Whats this?

```
Received: from mail-wi0-f169.google.com (mail-wi0-f169.google.com
[209.85.212.169])
        by mail.mailinator.com with SMTP (Postfix)
        for sam@mailinator.com;
        Thu, 04 Apr 2013 22:23:00 +0000 (UTC)
Received: by mail-wi0-f169.google.com with SMTP id c10so1234382wiw.0
        for <sam@mailinator.com>; Thu, 04 Apr 2013 15:22:59 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=mime-version:x-received:date:message-id:subject:from:to
         :content-type;
        bh=A1BTb7tga5RifOl556PHPyr9q1NOYQC58fYjGlKdOKg=;
        b=C7yuEtFFvUiHfGFomKtxdMFfdq27IXrGrsNhsuh097fqtStg6HTPVVbXxFcEx2XoTD
         MCdDGoFz6kk81Qwj+1PjhTOxsiV55RWiLQteRbKnjyiv50uIGyXjWogsm+HarFHpaaJo
         lu4sXY93RDltjgO+K3D4uf9JE84S+JoysV3Oe6KiQUqX7qJxXAfozNYwFDEZ+hUShcrg
         Jc6MiMZTczFl5MtwPif8FRALtl23TnOibwsdkjQXWCNbdYkvfPkwGvgyoJAsvvWm8jrj
         UvycQw8BikpQtkd/uQPsB2nQpZ1cuctPtte96N6w5XggmgNY2vmLZutMBcY5R/9oMZji
         Crcg==
MIME-Version: 1.0
X-Received: by 10.180.39.207 with SMTP id r15mr190931wik.16.1365114179203;
 Thu, 04 Apr 2013 15:22:59 -0700 (PDT)
Received: by 10.227.94.198 with HTTP; Thu, 4 Apr 2013 15:22:59 -0700 (PDT)
Date: Thu, 4 Apr 2013 15:22:59 -0700
Message-ID: <CAD=M77iw2iW0djDEUP_PxpEGfHsSowF1hs-m0Pk7Uuk4ezD49w@mail.gmail.com>
Subject: DEMO OF MAILINATOR
From: Sam Bowne <sam.bowne@gmail.com>
To: sam@mailinator.com
Content-Type: multipart/alternative; boundary=001a11c23f30babc6604d990698b

--001a11c23f30babc6604d990698b
Content-Type: text/plain; charset=ISO-8859-1
```

TRACING EMAIL

- ID pesan unik
- Membuktikan bahwa email telah melewati server
- Mendeteksi email dipalsukan

```
X-Received: by 10.180.39.207 with SMTP id r15mr190931wik.16.1365114179203;
 Thu, 04 Apr 2013 15:22:59 -0700 (PDT)
Received: by 10.227.94.198 with HTTP; Thu, 4 Apr 2013 15:22:59 -0700 (PDT)
Date: Thu, 4 Apr 2013 15:22:59 -0700
Message-ID: <CAD=M77iw2iW0djDEUP_PxpEGfHsSowF1hs-m0Pk7Uuk4ezD49w@mail.gmail.com>
Subject: DEMO OF MAILINATOR
From: Sam Bowne <sam.bowne@gmail.com>
To: sam@mailinator.com
```

SOCIAL NETWORKING

OVER-SHARING

- Orang bisa terus berbincang dan sharing sesuatu
- Facebook
- Twitter
- FourSquare
  - Orang check-in dengan lokasi mereka saat ini
- Bukti bisa terdapat pada komputer tersangka, smartphone atau provider

COMPLIANCE GUIDE FOR
LAW ENFORCEMENT

- Basic subscriber records: approx. $20 for the first ID, $10 per ID thereafter
- Basic Group Information (including information about moderators): approx. $20 for a group with a single moderator
- Contents of subscriber accounts, including email: approx. $30-$40 per user
- Contents of Groups: approx. $40 - $80 per group

Link Ch 8n: Yahoo Compliance Guide for Law Enforcement

DATA AVAILABILITY AT A GLANCE

Record Type	Accessible for?	Purged After?
Subscriber Information	As long as account is active	18 months of inactivity or 90 days if subscriber self-deletes account
Account Log-in IP addresses	Up to one year	N/A
Email (free or premium)	As long as user chooses to keep it	4 or more months of inactivity depending on how long user's account was open
Flickr Account Contents, including Flickr Email	As long a account is active (Email stored as long as user chooses to keep it)	Upon deactivation of account
Groups – Activity Logs	Life of the Group	Minimum of 30 days after termination of Group
Groups – Content	Life of the Group (only current version of Group stored; not past versions)	Minimum of 30 days after termination of Group
Chat/Instant Messenger Logs	45-60 days	N/A
Web Messenger Contents (Yahoo! does not store contents of communications sent via the downloadable Messenger client)	As long as user chooses to keep it	N/A
GeoCities, Domains, Web-hosting – Activity Logs and Content	As long as website or domain is active	Minimum of 30 days after termination of website or domain
Profiles	As long as the Profile is active	Minimum of 90 days after deactivation