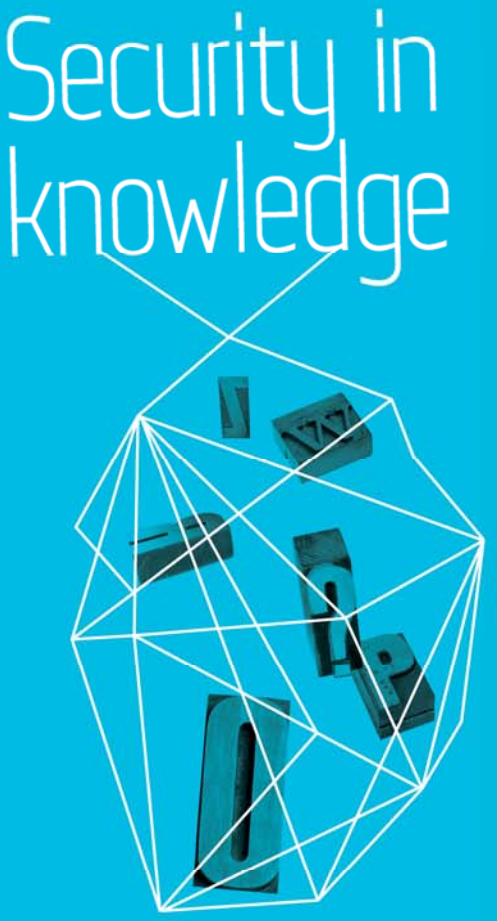
RSA CONFERENCE ASIA PACIFIC 2013



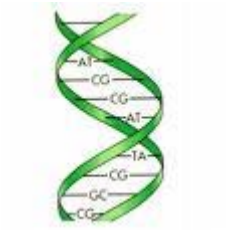
THE FUTURE OF DIGITAL FORENISCS

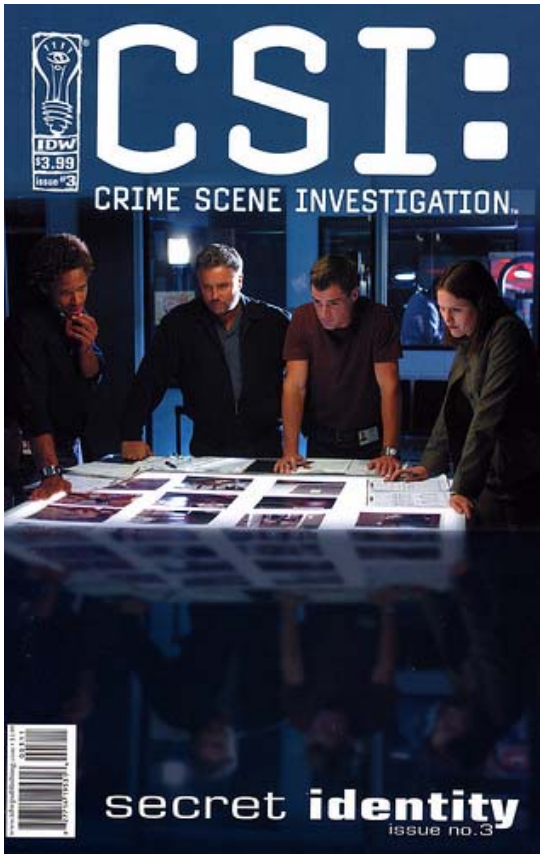
SungKyong Un
ETRI

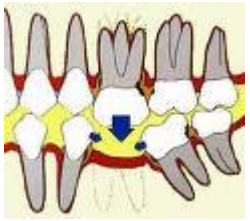
Session ID: CLE-W04

Session Classification: Intermediate

Forensics







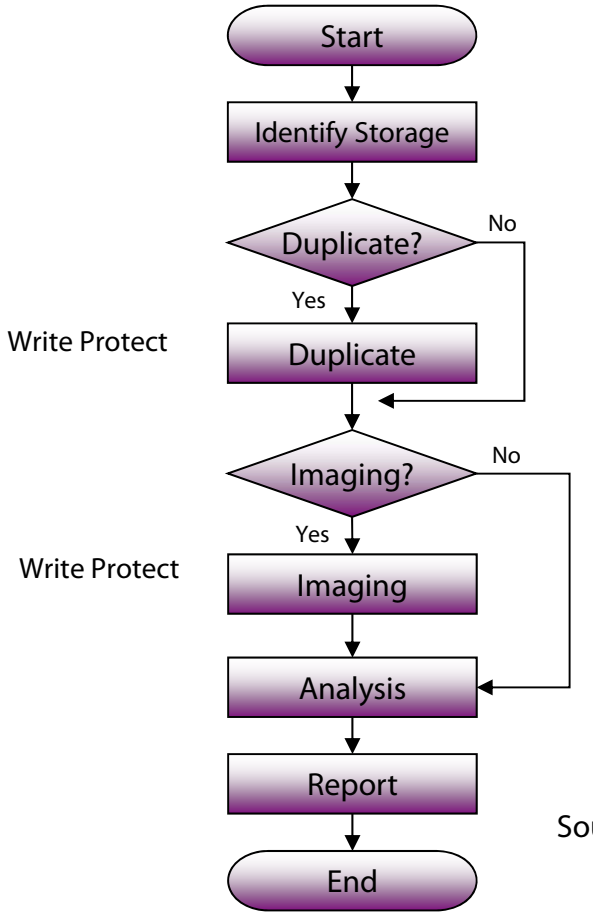
Source: mlhradio@flickr

Digital Forensics

Digital Forensics

- DFRWS (2001) defines
  - The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

Digital Forensics Procedure



Source : TTAS.KO-12.0058

"Computer Forensics Guideline"

Imaging

HDD Imaing
source : joncrel@flickr

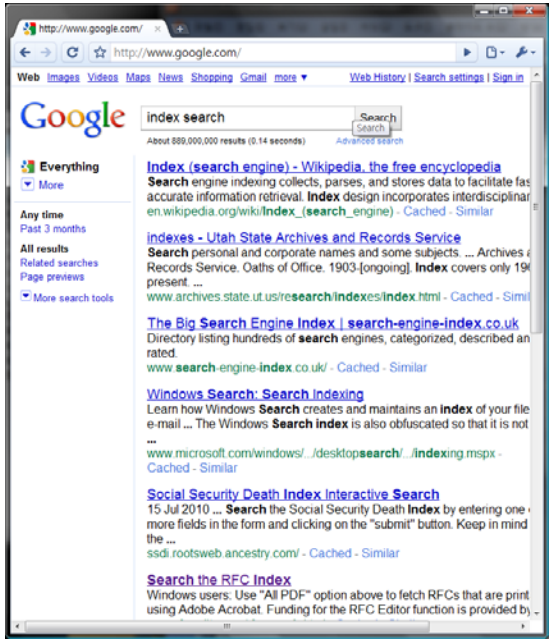
Hardware Duplicator
source: http://www.solstice-inc.com

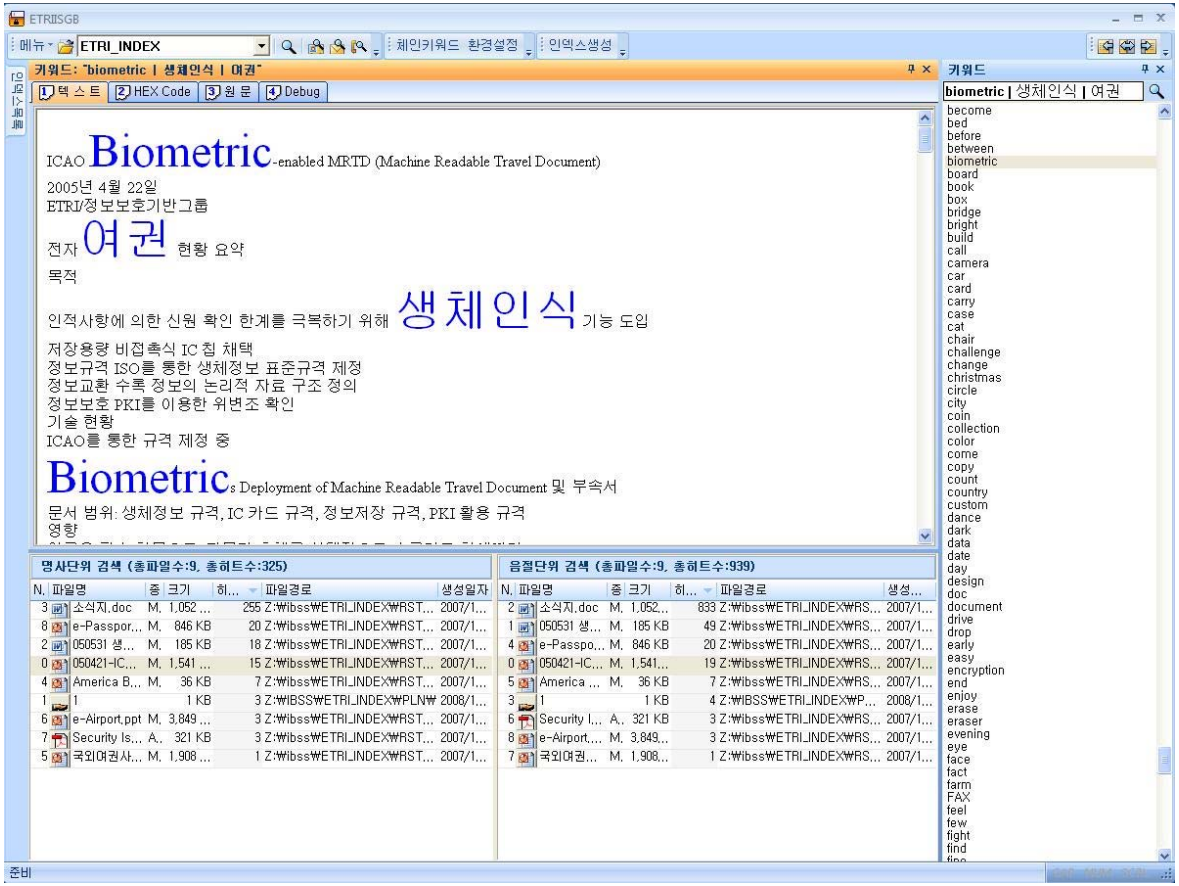
Recovery

Keyword Search

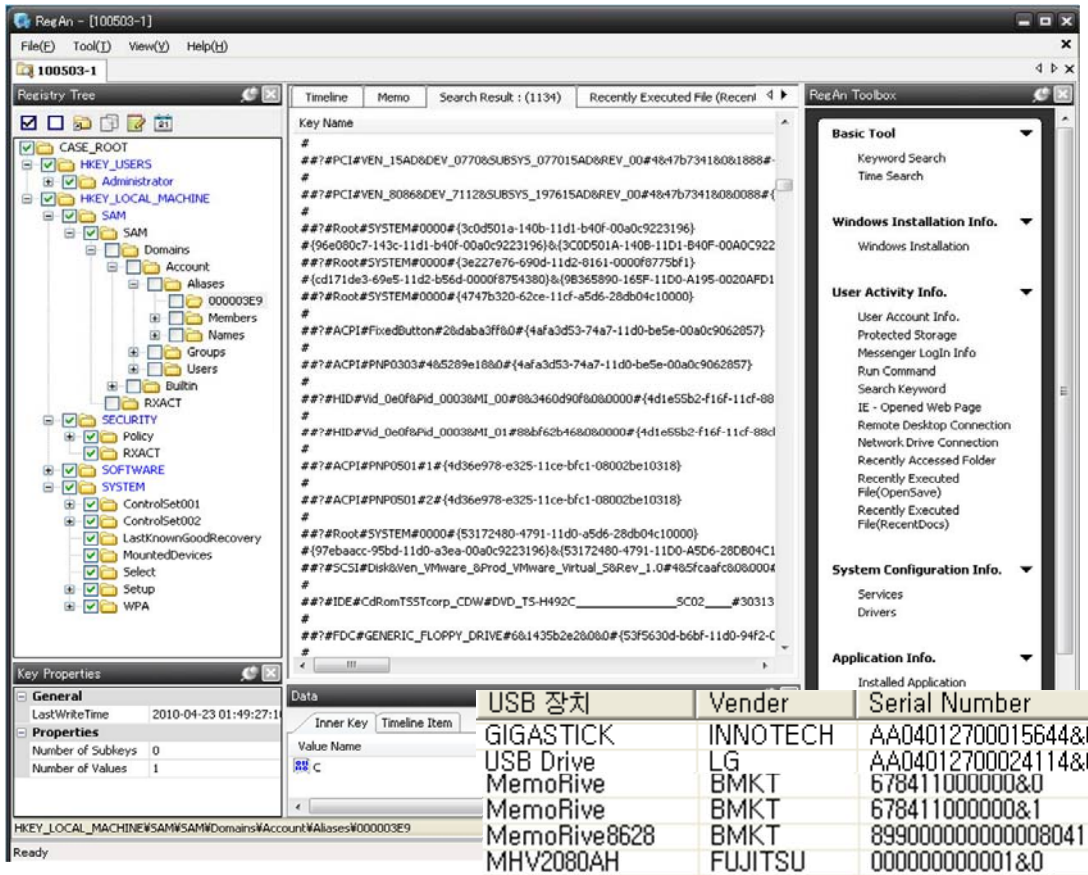
source : Konrad Andrews@flickr

Index Search





Registry

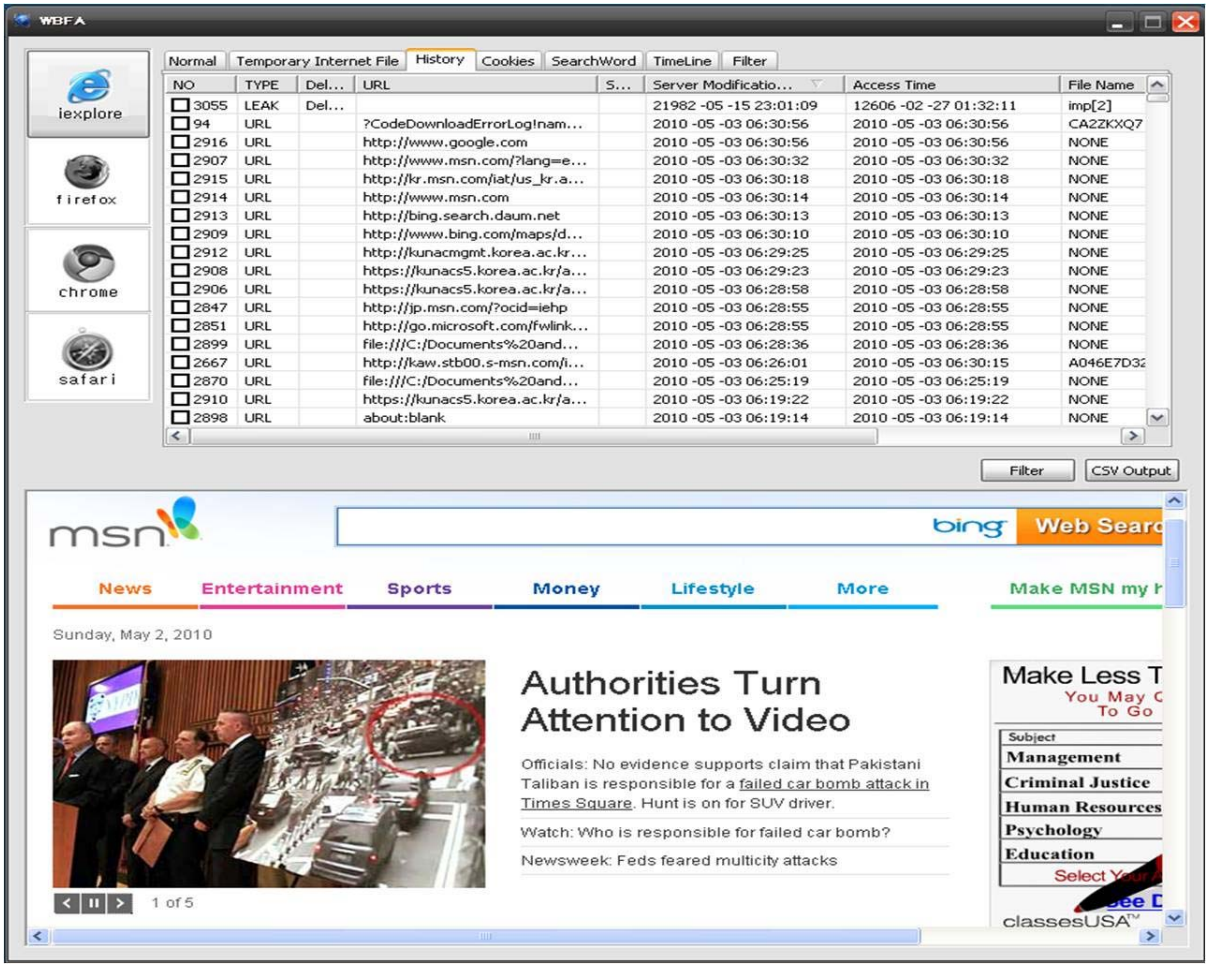


USB 장치	Vender	Serial Number	First Connected Time	Device Type
GIGASTICK	INNOTECH	AA040127000156448&0	2009-02-25 23:28:59	CD 드라이브
USB Drive	LG	AA040127000241148&0	2009-06-11 01:16:33	CD 드라이브
MemoRive	BMKT	678411000000&0	2009-03-02 13:50:49	이동식 디스크
MemoRive	BMKT	678411000000&1	2009-03-02 13:50:49	이동식 디스크
MemoRive8628	BMKT	899000000000008041108 3D6...	2009-02-25 23:29:46	이동식 디스크
MHV2080AH	FUJITSU	000000000001&0	2009-08-08 21:55:34	이동식 디스크
MHX2300BT	FUJITSU	2018128AC888&0	2009-03-09 10:49:11	이동식 디스크
Atom	Imation	AA6270851160000000 91&0	2009-03-13 21:36:07	이동식 디스크
GIGASTICK	INNOTECH	AA040127000156448&1	2009-02-25 23:28:59	이동식 디스크

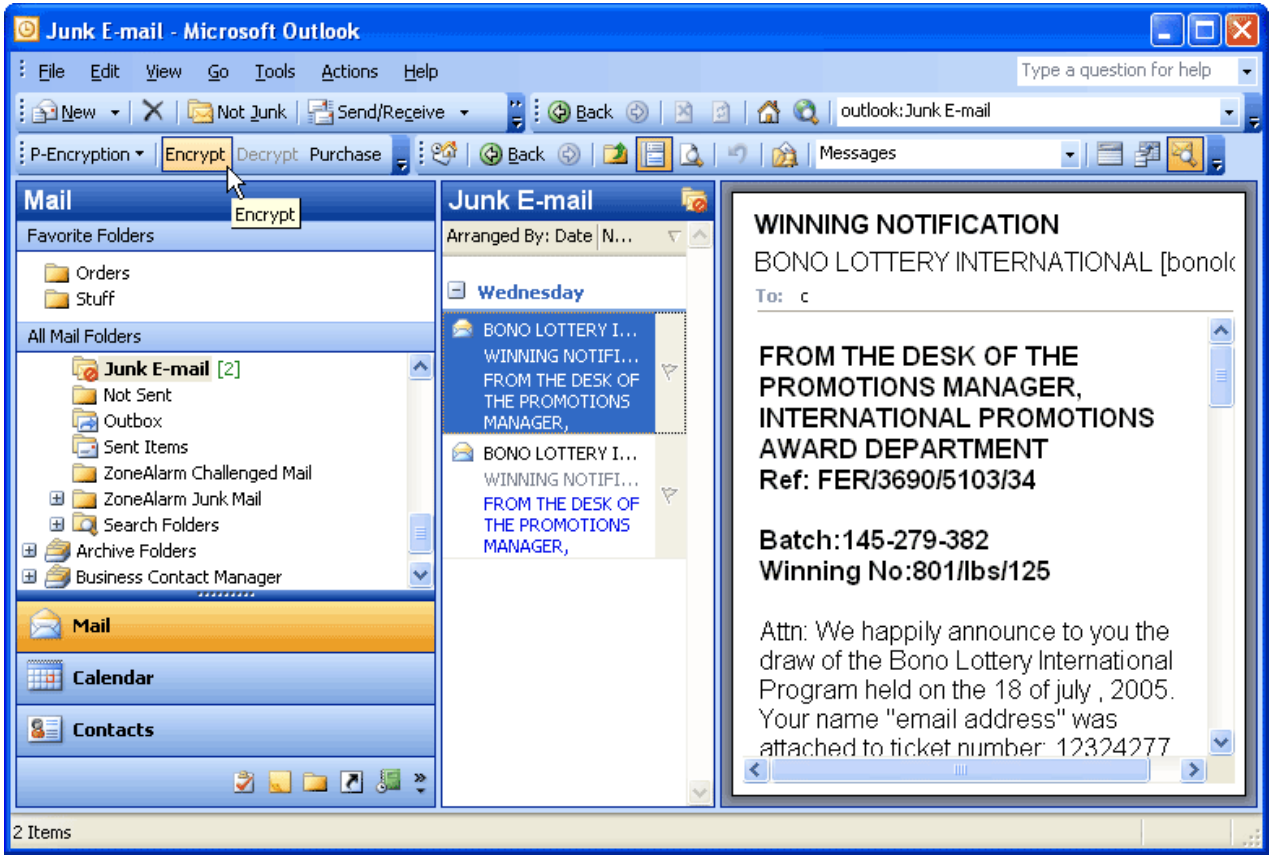
Web History

mozilla Firefox®

Google Chrome



Email


Junk E-mail - Microsoft Outlook
File Edit View Go Tools Actions Help
Type a question for help
New
Not Junk
Send/Receive
Back
outlook:Junk E-mail
P-Encryption
Encrypt
Decrypt
Purchase
Back
Messages
Encrypt
Mail
Favorite Folders
Orders
Stuff
All Mail Folders
Junk E-mail [2]
Not Sent
Outbox
Sent Items
ZoneAlarm Challenged Mail
ZoneAlarm Junk Mail
Search Folders
Archive Folders
Business Contact Manager
Mail
Calendar
Contacts
Junk E-mail
Arranged By: Date
Wednesday
BONO LOTTERY I...
WINNING NOTIFI...
FROM THE DESK OF THE PROMOTIONS MANAGER,
BONO LOTTERY I...
WINNING NOTIFI...
FROM THE DESK OF THE PROMOTIONS MANAGER,
WINNING NOTIFICATION
BONO LOTTERY INTERNATIONAL [bonol
To: c
FROM THE DESK OF THE PROMOTIONS MANAGER, INTERNATIONAL PROMOTIONS AWARD DEPARTMENT
Ref: FER/3690/5103/34
Batch:145-279-382
Winning No:801/lbs/125
Attn: We happily announce to you the draw of the Bono Lottery International Program held on the 18 of july , 2005. Your name "email address" was attached to ticket number: 12324277
2 Items

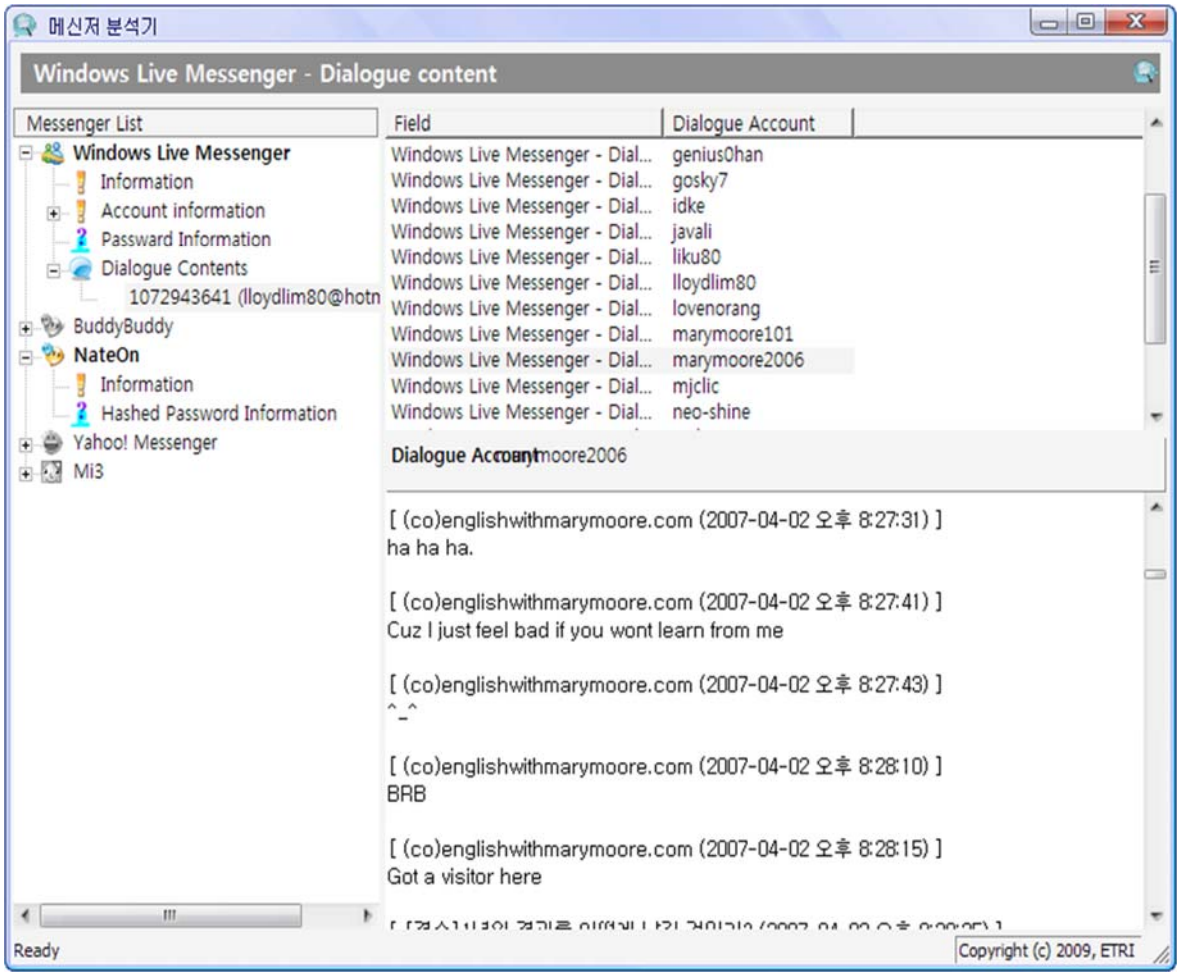
Messenger


Windows Live Messenger


buddy
BUDDY


NateOn


Mi3


메신저 분석기
Windows Live Messenger - Dialogue content
Messenger List
Windows Live Messenger
Information
Account information
Password Information
Dialogue Contents
1072943641 (lloydlim80@hotn
BuddyBuddy
NateOn
Information
Hashed Password Information
Yahoo! Messenger
Mi3
Field
Dialogue Account
Windows Live Messenger - Dial... geniusOhan
Windows Live Messenger - Dial... gosky7
Windows Live Messenger - Dial... idke
Windows Live Messenger - Dial... javali
Windows Live Messenger - Dial... liku80
Windows Live Messenger - Dial... lloydlim80
Windows Live Messenger - Dial... lovenorang
Windows Live Messenger - Dial... marymoore101
Windows Live Messenger - Dial... marymoore2006
Windows Live Messenger - Dial... mjclic
Windows Live Messenger - Dial... neo-shine
Dialogue Account: marymoore2006
[(co)englishwithmarymoore.com (2007-04-02 오후 8:27:31)]
ha ha ha.
[(co)englishwithmarymoore.com (2007-04-02 오후 8:27:41)]
Cuz I just feel bad if you wont learn from me
[(co)englishwithmarymoore.com (2007-04-02 오후 8:27:43)]
^_^
[(co)englishwithmarymoore.com (2007-04-02 오후 8:28:10)]
BRB
[(co)englishwithmarymoore.com (2007-04-02 오후 8:28:15)]
Got a visitor here
Ready
Copyright (c) 2009, ETRI

Anti-Forensics - Eraser

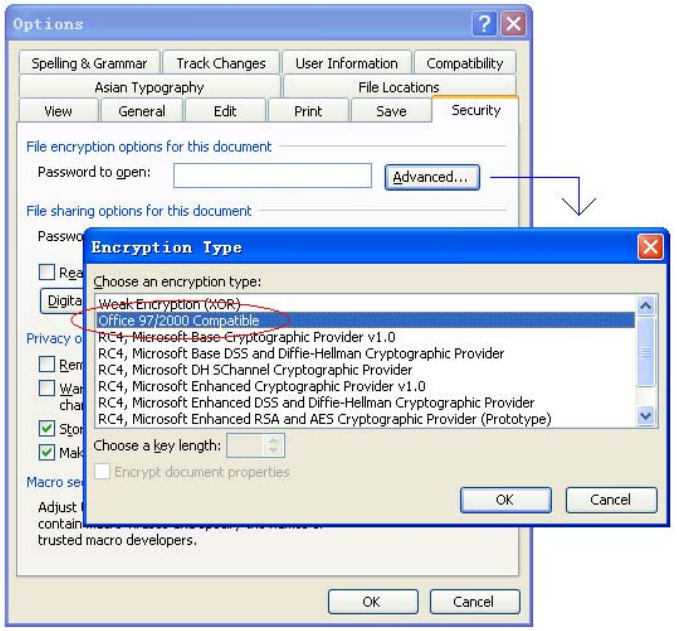
Automatic Eraser
source: http://www.wiebetech.com

Magnatic Eraser
source: http://www.garner-product.com

Anti-Forensics - Encryption

MS BitLocker
Drive Encryption (AES)
Windows Vista, 7

Apple FileVault
Encrypted File System (AES)
Mac OS X v10.3



MS Office Encryption Option
Various Algorithm

Anti-Forensics - Countermeasure

GPU based parallel password search
Source : ETRI

FPGA based password search
Source : www.tableau.com

RSA CONFERENCE ASIA PACIFIC 2013

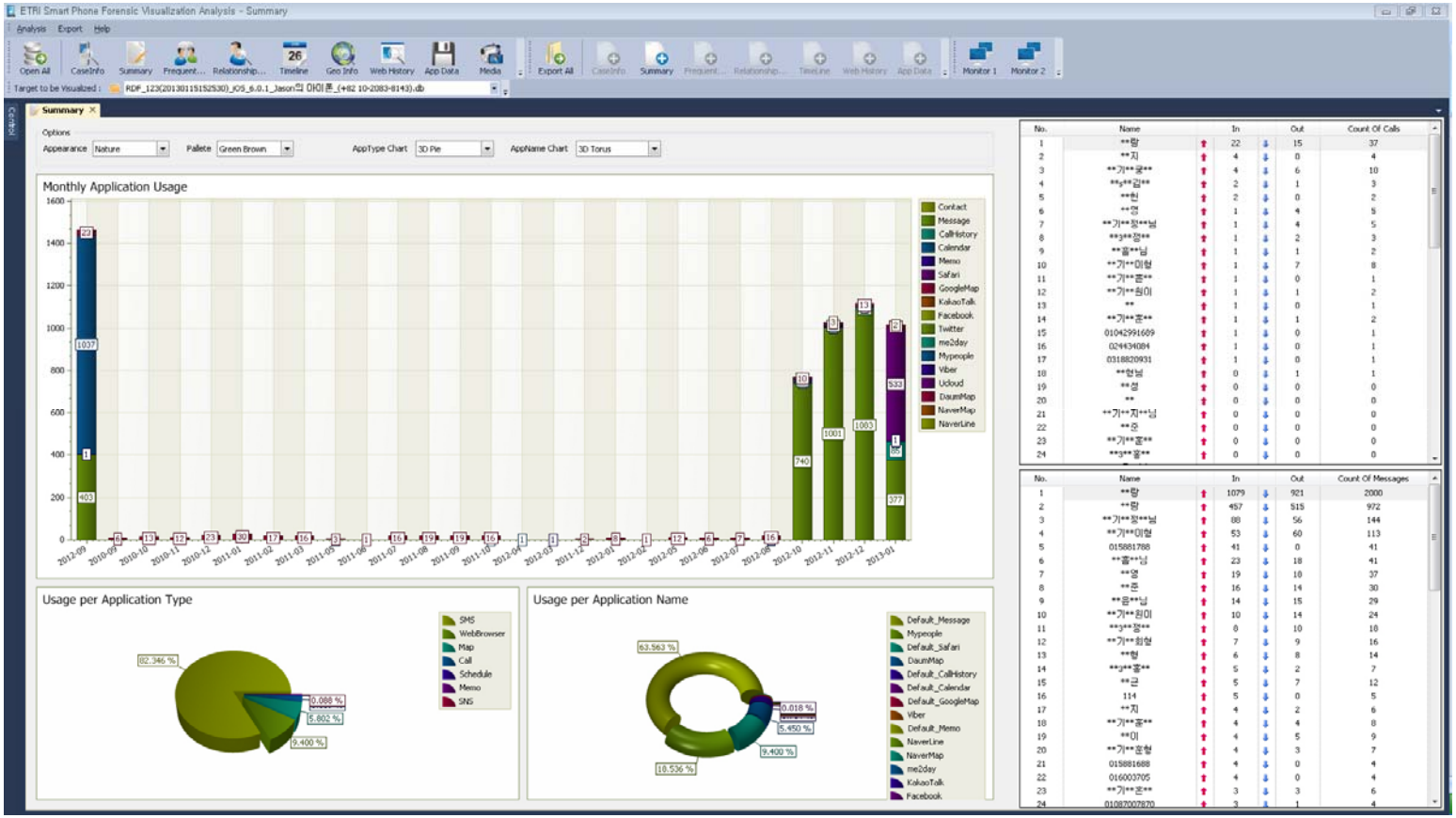
The Present

SmartPhone Forensics

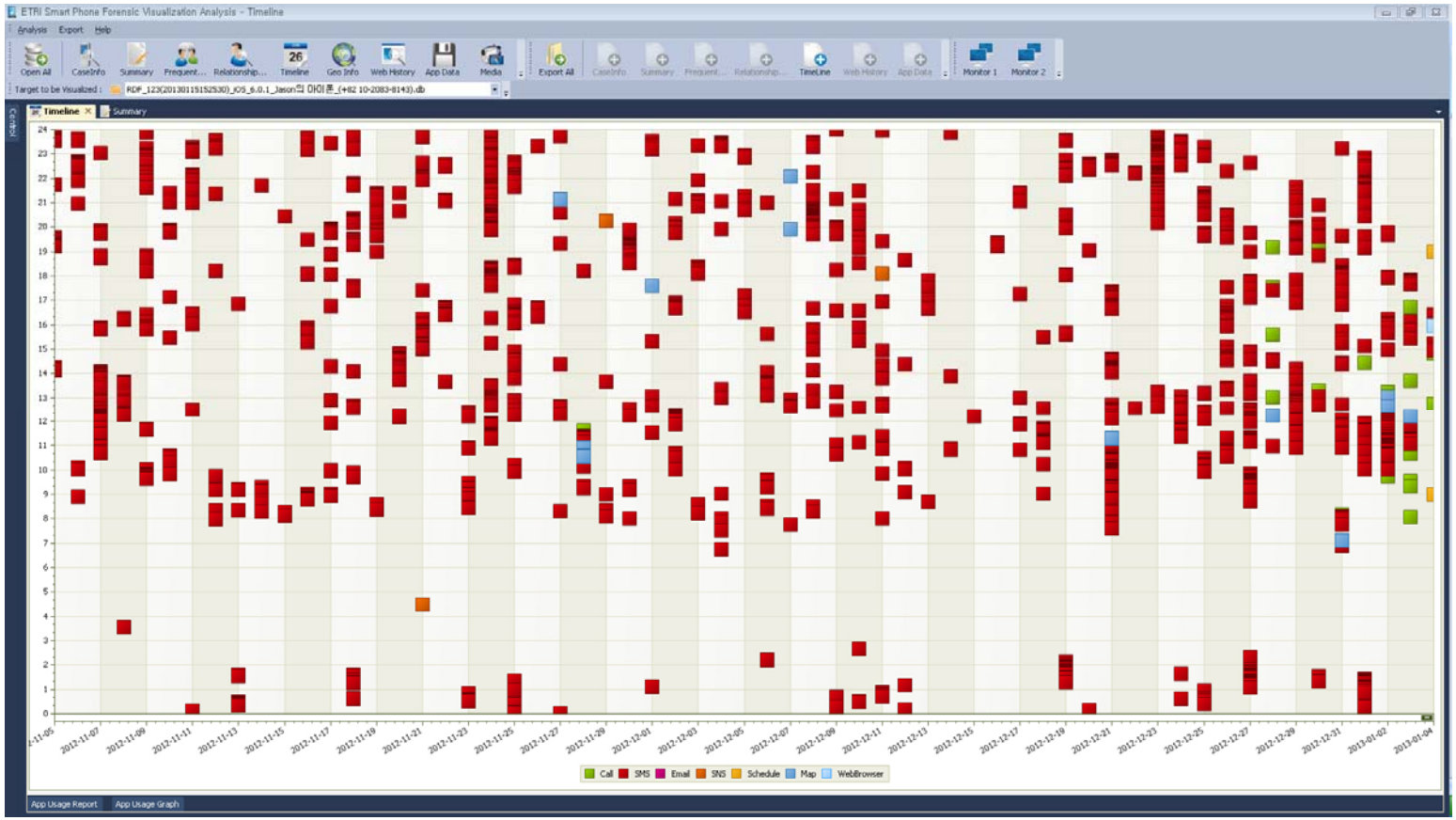
SmartPhone Forensics

Item	Dummy	Smart
Target Models	>1,000/Year	>10/Year
OS	Symbian, Qualcomm	iOS, Android, Windows Mobile, BlackberryOS
Interface	Various	USB
Acquisition	Logical, Physical	Logical, Physical, Backup
Data	Phone book, Call history, SMS, Photo, Schedule	+ Email, Web History, Map, Location, SNS, Message, App, ID/PW
DB Format	Various	Sqlite
3rd Party App	-	App Market

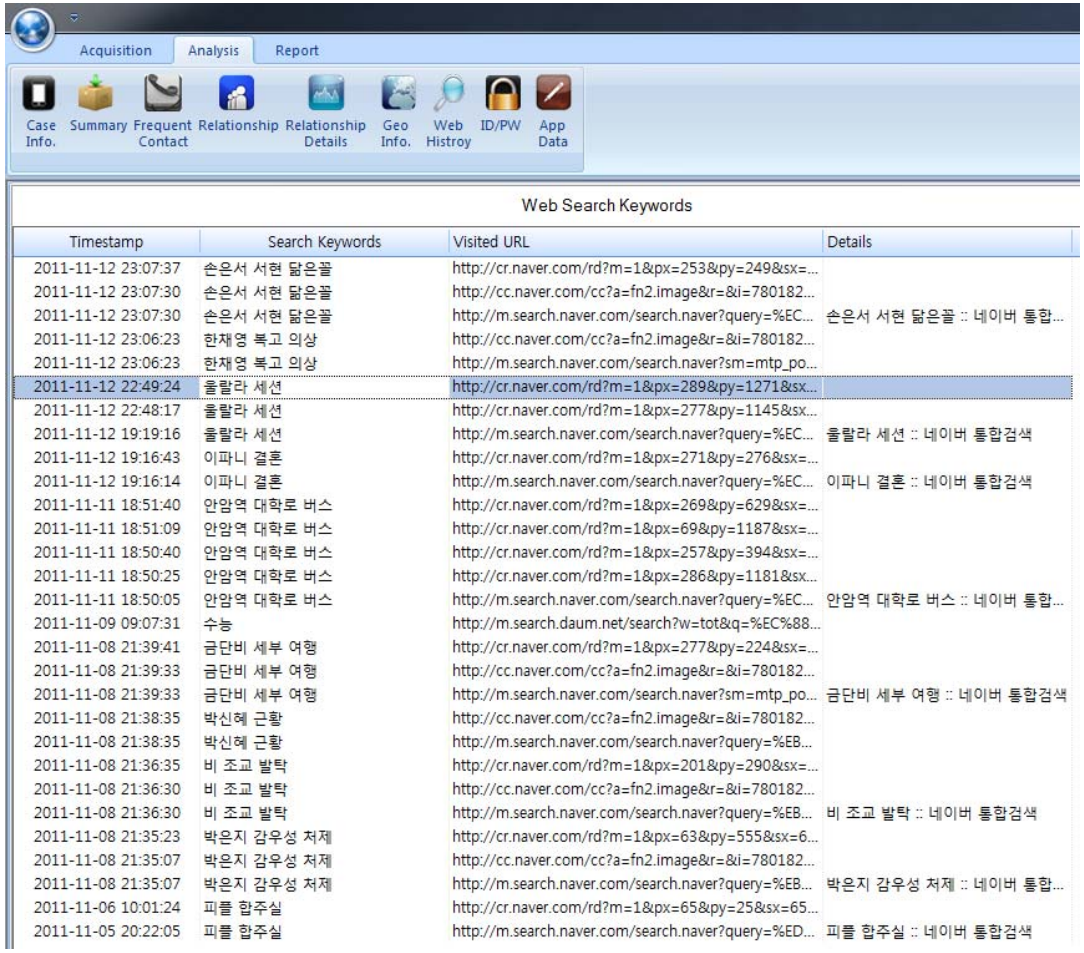
Analysis - Briefing



Analysis - Timeline



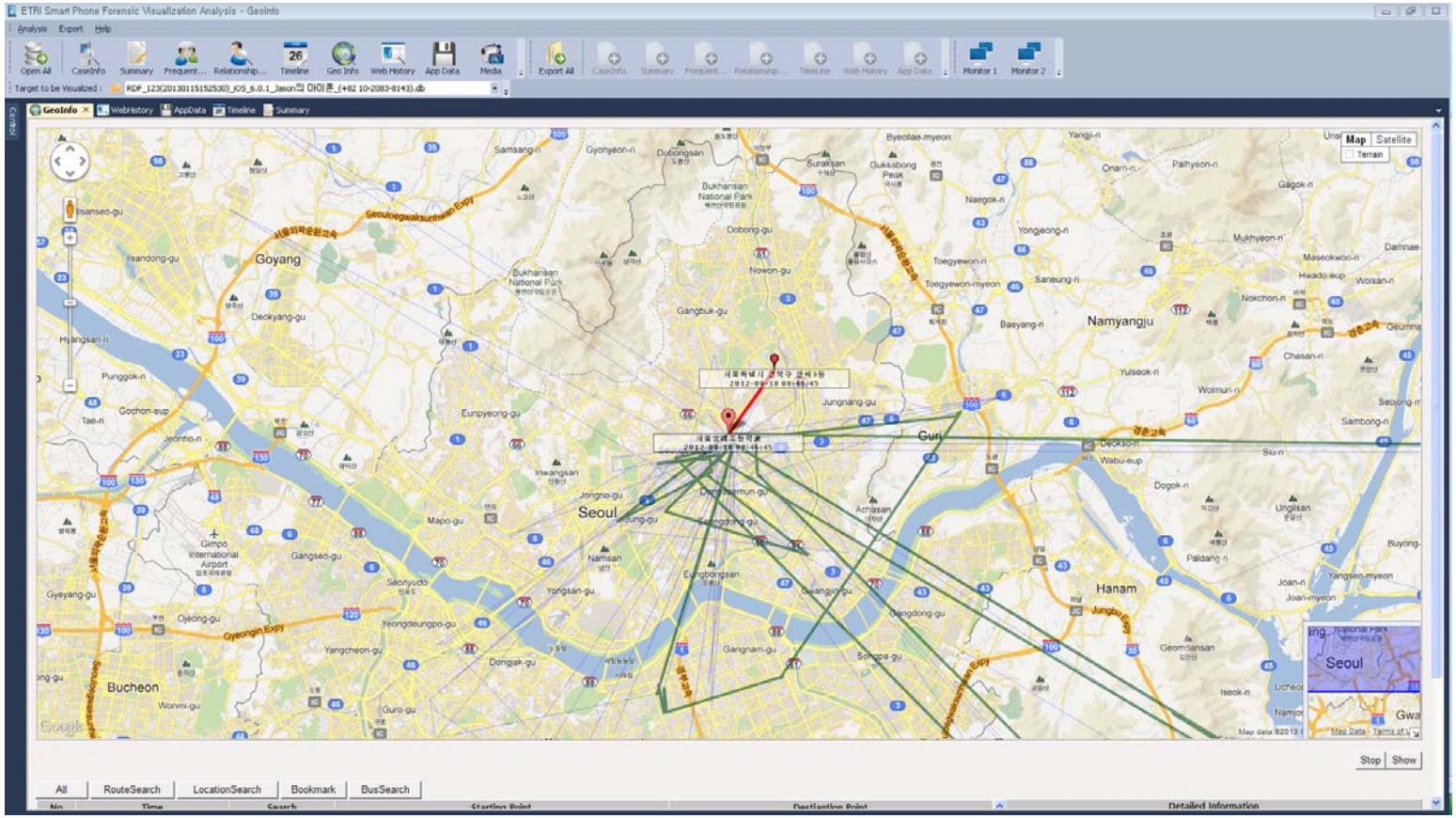
Analysis – Web Browsing



Web Search Keywords

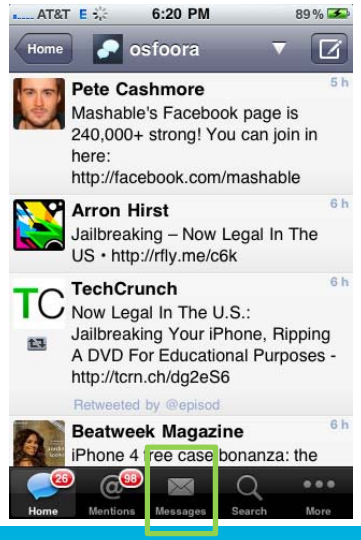
Timestamp	Search Keywords	Visited URL	Details
2011-11-12 23:07:37	손은서 서현 닮은꼴	http://cr.naver.com/rd?m=1&px=253&py=249&sx=...	
2011-11-12 23:07:30	손은서 서현 닮은꼴	http://cc.naver.com/cc?a=fn2.image&r=&i=780182...	
2011-11-12 23:07:30	손은서 서현 닮은꼴	http://m.search.naver.com/search.naver?query=%EC...	손은서 서현 닮은꼴 :: 네이버 통합...
2011-11-12 23:06:23	한채영 복고 의상	http://cc.naver.com/cc?a=fn2.image&r=&i=780182...	
2011-11-12 23:06:23	한채영 복고 의상	http://m.search.naver.com/search.naver?sm=mtp_po...	
2011-11-12 22:49:24	울랄라 세션	http://cr.naver.com/rd?m=1&px=289&py=1271&sx...	
2011-11-12 22:48:17	울랄라 세션	http://cr.naver.com/rd?m=1&px=277&py=1145&sx...	
2011-11-12 19:19:16	울랄라 세션	http://m.search.naver.com/search.naver?query=%EC...	울랄라 세션 :: 네이버 통합검색
2011-11-12 19:16:43	이파니 결혼	http://cr.naver.com/rd?m=1&px=271&py=276&sx=...	
2011-11-12 19:16:14	이파니 결혼	http://m.search.naver.com/search.naver?query=%EC...	이파니 결혼 :: 네이버 통합검색
2011-11-11 18:51:40	안암역 대학로 버스	http://cr.naver.com/rd?m=1&px=269&py=629&sx=...	
2011-11-11 18:51:09	안암역 대학로 버스	http://cr.naver.com/rd?m=1&px=69&py=1187&sx=...	
2011-11-11 18:50:40	안암역 대학로 버스	http://cr.naver.com/rd?m=1&px=257&py=394&sx=...	
2011-11-11 18:50:25	안암역 대학로 버스	http://cr.naver.com/rd?m=1&px=286&py=1181&sx...	
2011-11-11 18:50:05	안암역 대학로 버스	http://m.search.naver.com/search.naver?query=%EC...	안암역 대학로 버스 :: 네이버 통합...
2011-11-09 09:07:31	수능	http://m.search.daum.net/search?w=tot&q=%EC%88...	
2011-11-08 21:39:41	금단비 세부 여행	http://cr.naver.com/rd?m=1&px=277&py=224&sx=...	
2011-11-08 21:39:33	금단비 세부 여행	http://cc.naver.com/cc?a=fn2.image&r=&i=780182...	
2011-11-08 21:39:33	금단비 세부 여행	http://m.search.naver.com/search.naver?sm=mtp_po...	금단비 세부 여행 :: 네이버 통합검색
2011-11-08 21:38:35	박신혜 근황	http://cc.naver.com/cc?a=fn2.image&r=&i=780182...	
2011-11-08 21:38:35	박신혜 근황	http://m.search.naver.com/search.naver?query=%EB...	
2011-11-08 21:36:35	비 조교 발탁	http://cr.naver.com/rd?m=1&px=201&py=290&sx=...	
2011-11-08 21:36:30	비 조교 발탁	http://cc.naver.com/cc?a=fn2.image&r=&i=780182...	
2011-11-08 21:36:30	비 조교 발탁	http://m.search.naver.com/search.naver?query=%EB...	비 조교 발탁 :: 네이버 통합검색
2011-11-08 21:35:23	박은지 감우성 처제	http://cr.naver.com/rd?m=1&px=63&py=555&sx=6...	
2011-11-08 21:35:07	박은지 감우성 처제	http://cc.naver.com/cc?a=fn2.image&r=&i=780182...	
2011-11-08 21:35:07	박은지 감우성 처제	http://m.search.naver.com/search.naver?query=%EB...	박은지 감우성 처제 :: 네이버 통합...
2011-11-06 10:01:24	피쿨 합주실	http://cr.naver.com/rd?m=1&px=65&py=25&sx=65...	
2011-11-05 20:22:05	피쿨 합주실	http://m.search.naver.com/search.naver?query=%ED...	피쿨 합주실 :: 네이버 통합검색

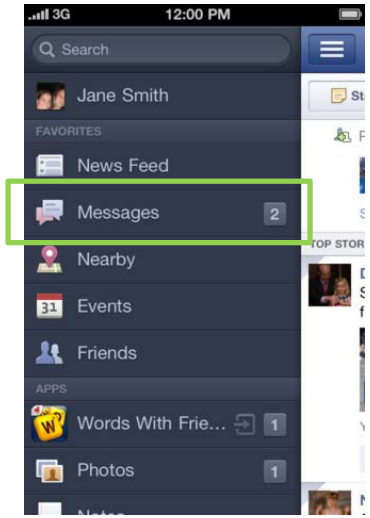
Analysis – Location & Routing



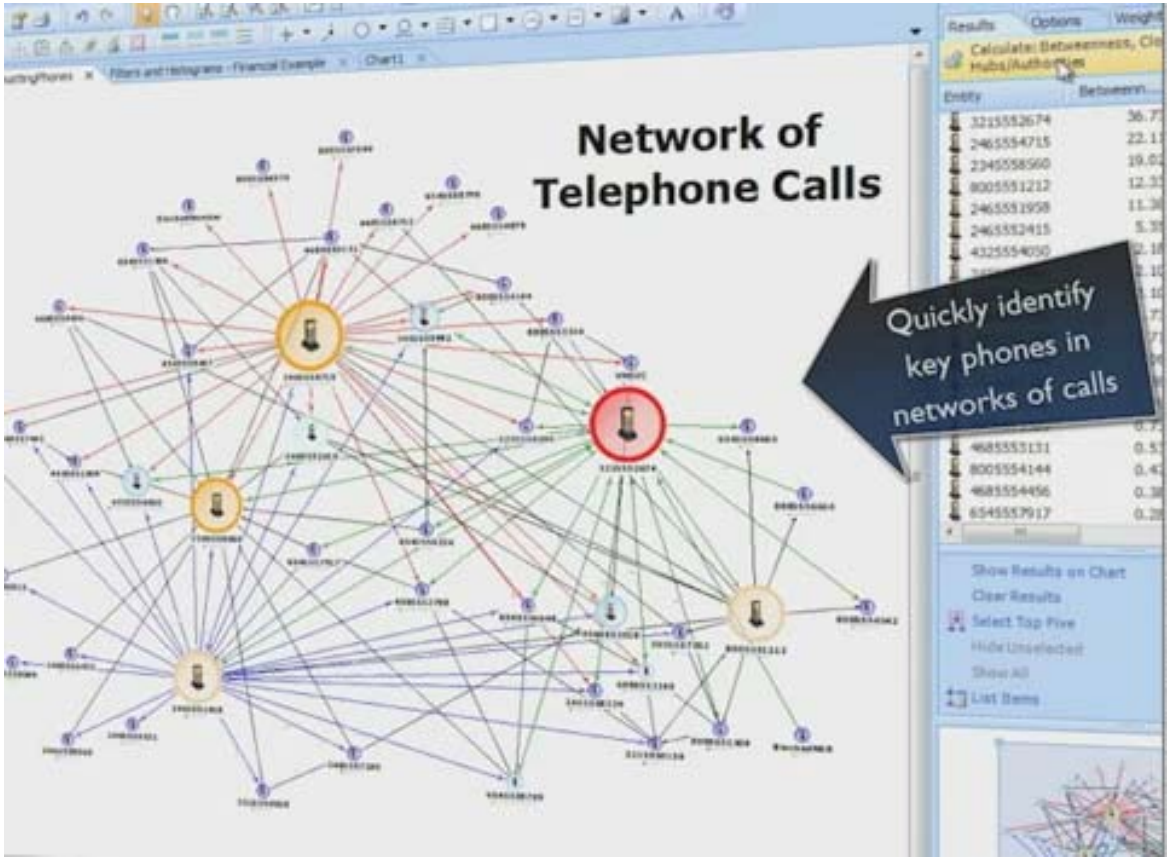
Analysis – App

Category	App
Phone Call	Skype, Viber, Google Voice, ...
Message	Cacao Talk, iMessage, Twitter DM, Facebook Message, ...
SNS	Twitter, Facebook, me2day, ...
Storage	Dropbox, uCloud, SugarSync, Box.net, iCloud, ...
Key	DataVault, 1Password, Strip, ...



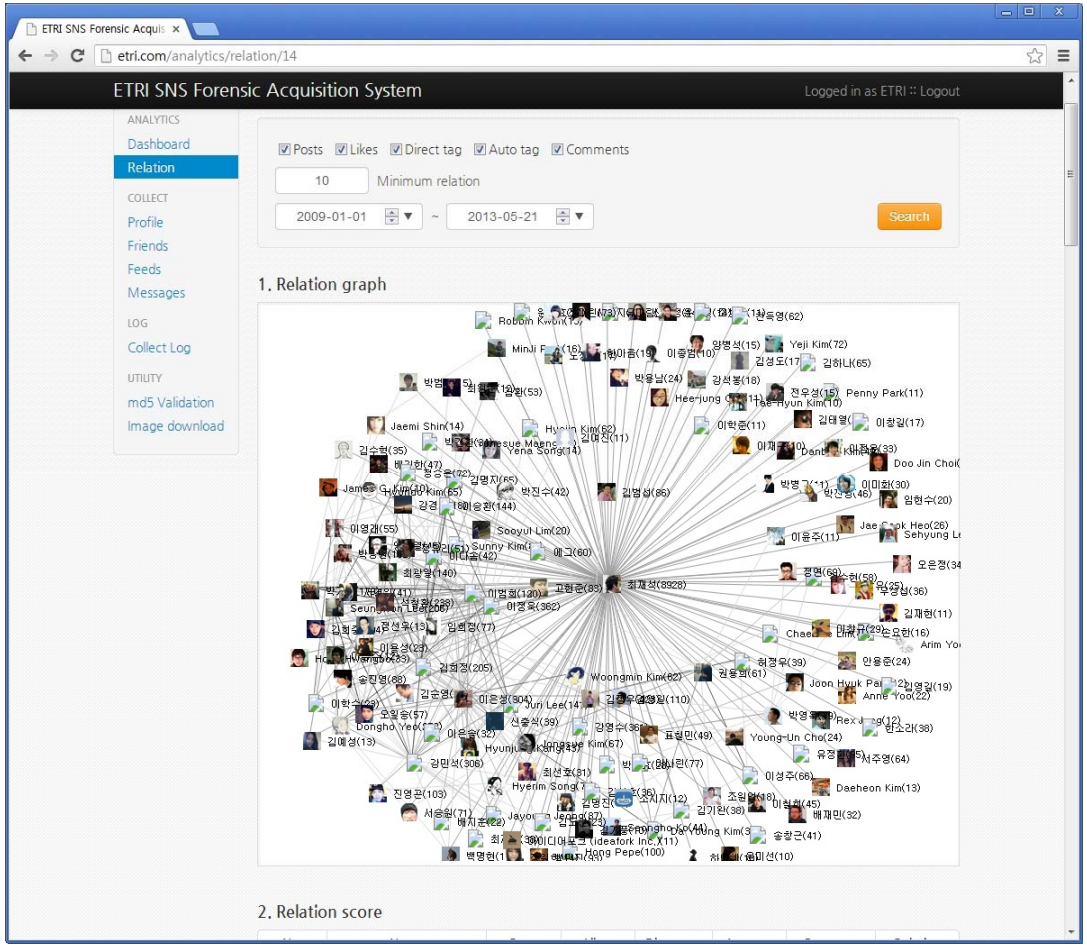


Analysis – Communication Network



source: http://www.i2group.com

Analysis – Social Network



RSA CONFERENCE ASIA PACIFIC 2013

The Future

Problem or Inconvience

Large Storage → Search Space++ → 1TB 14H? (20MB/s)

New Device/Service → New Tools → Buy/Educate? → Forensics= Tool Expert?

New Environment → Internet (Blog,Cafe, SNS) → Cloud Computing (Seizure & Search Warrant?) → Smart Phone

Binary Search → Index Search → What if keyword is not known?

New Viewpoint

Investigating the case, not the device → Need information, not data

Multiple device/services per user → Need multi(source) data integration

Continuous device/service creation/change → Need a framework to host

Multiple remote sites → Need mobility & connectivity

Volatile evidences → Need acquisition method & third party attestation

The Future of Digital Forensics

Data Centric Analysis → Conduct Centric Analysis

Forensic Tools → Forensic Services

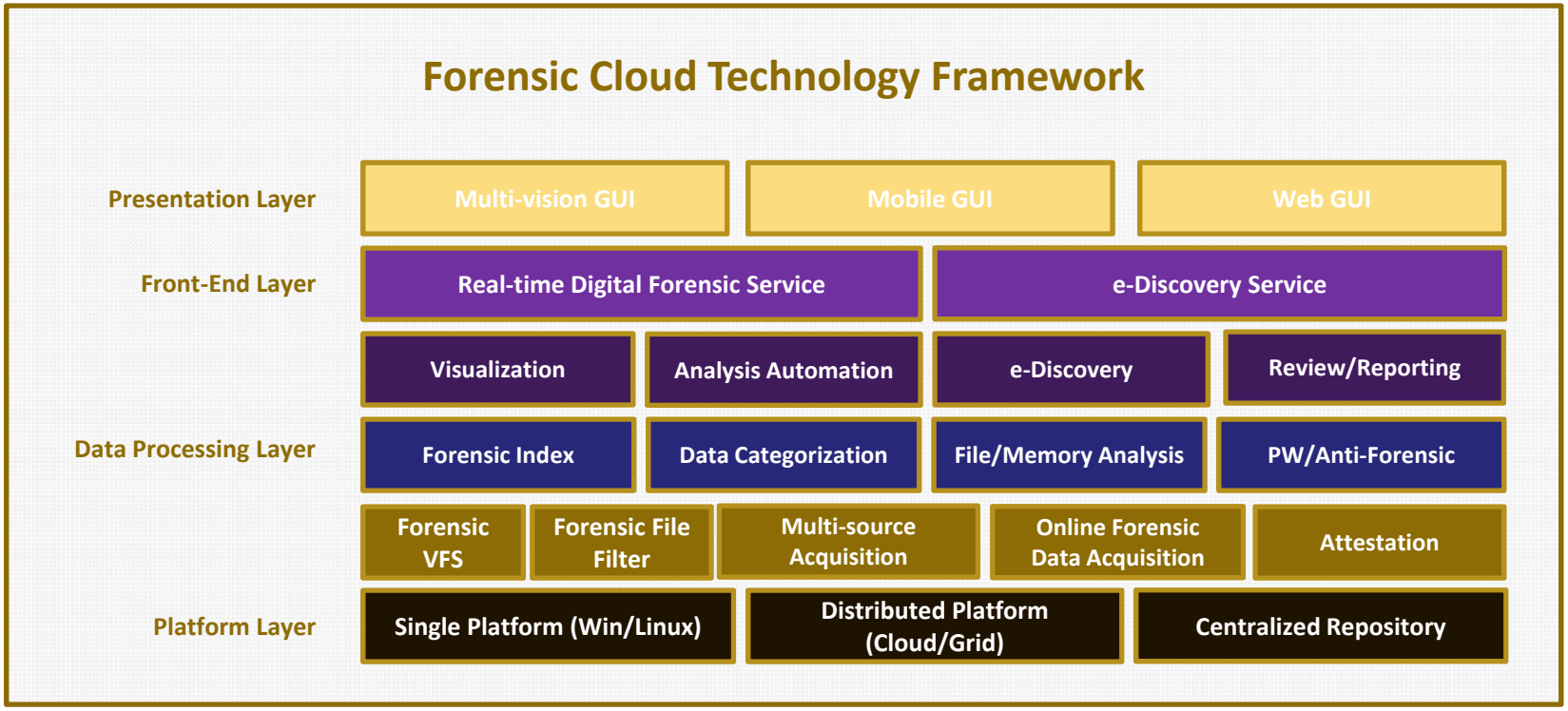
Conduct Centric Analysis

- Multi-source Evidence Acquisition
- Relationship Analysis
- Intuitive Analysis
- Automatic Analysis Based on the Profile

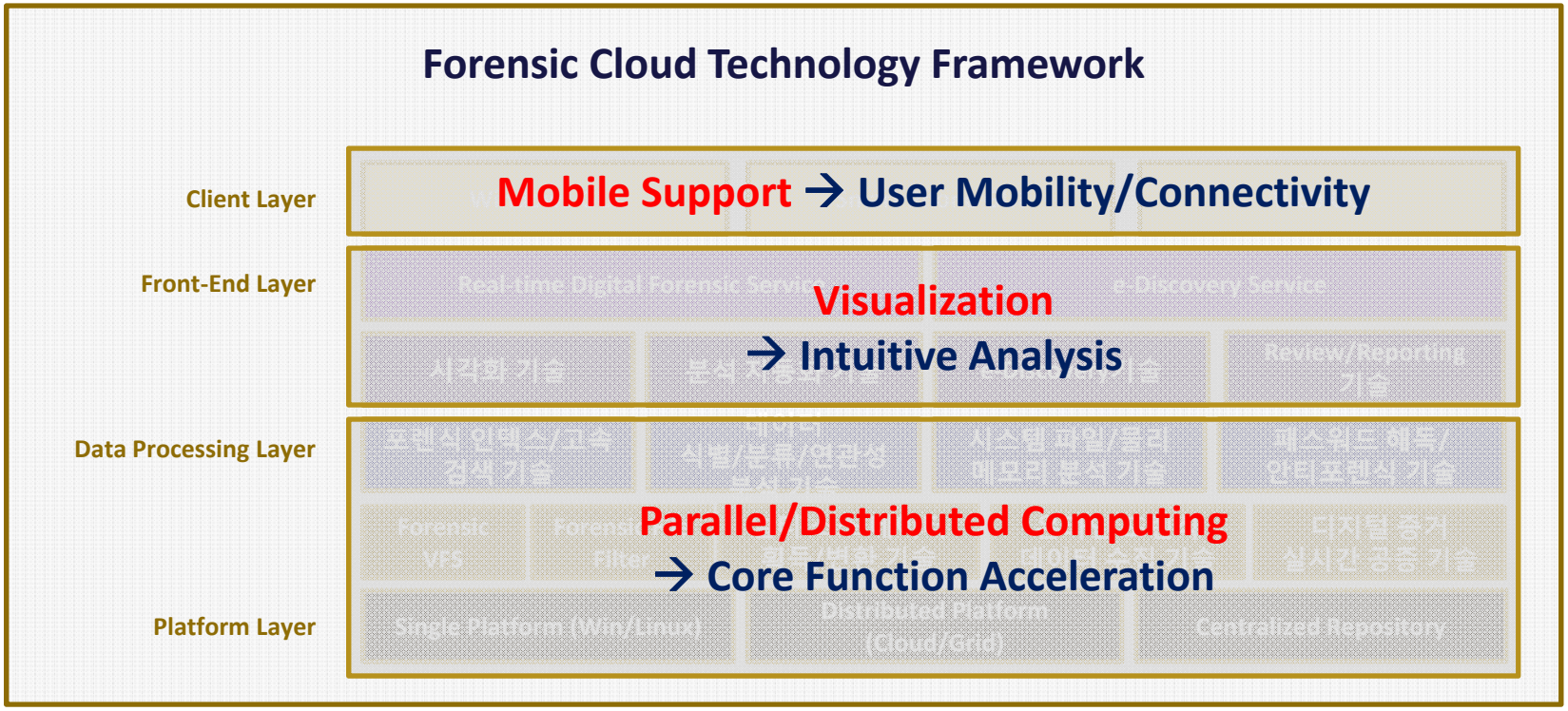
Forensic Services

- Parallel/Distributed Platform for Large Data Handling
- Adapting Fast Changing Device/Tools
- User Mobility & Connectivity

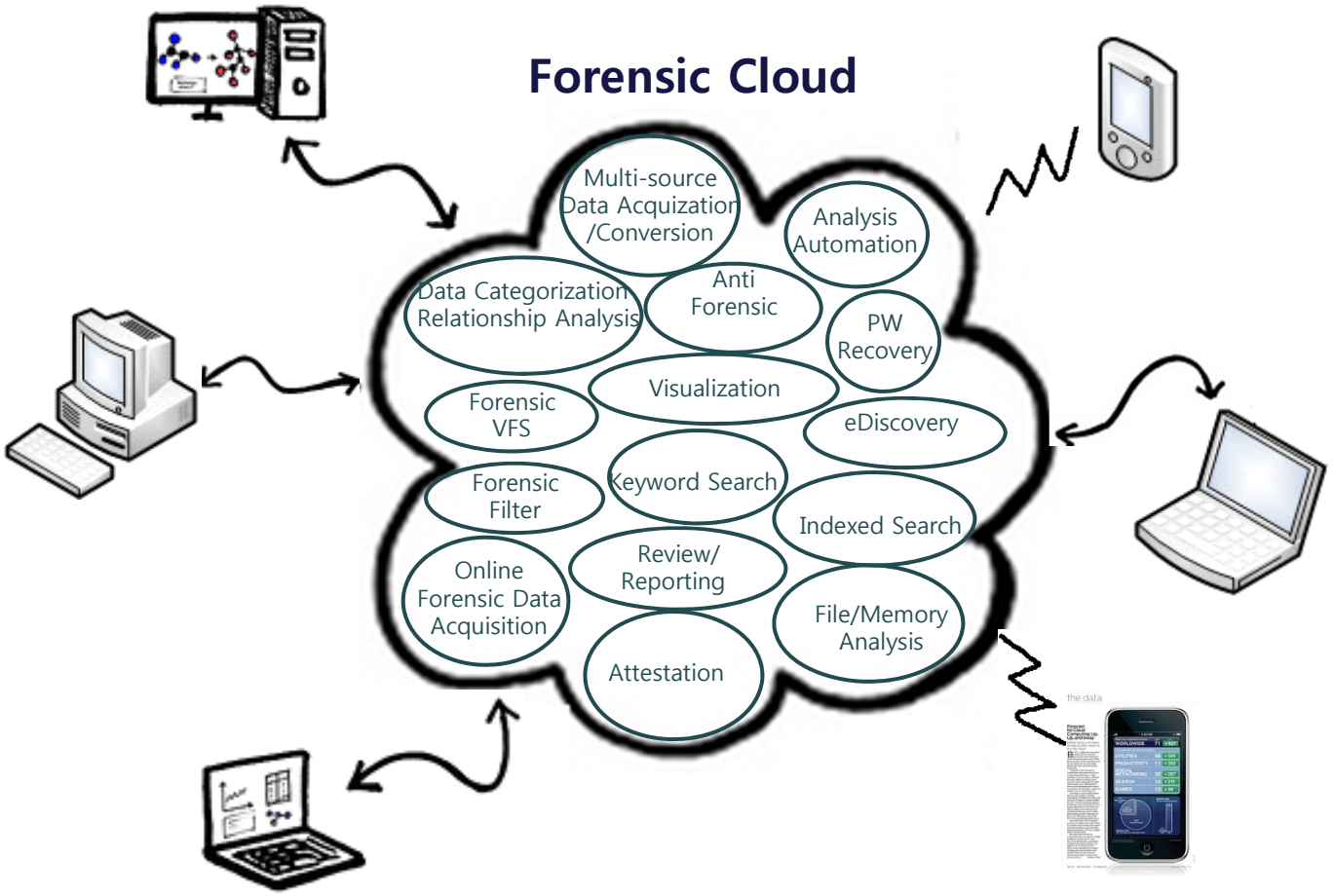
Forensic Cloud: Forensics as a Service



Forensic Cloud: Forensics as a Service



Forensic Cloud: Forensics as a Service



Forensic Cloud: Forensics as a Service

source: http://en.wikipedia.org/wiki/File:Sun_Modular_Datacenter_SunEBC.JPG