Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

July 06, 2011

Virginia Information Technologies Agency

ISOAG July 2011 Agenda

I.	Welcome & Opening Remarks	John Green, VITA
II.	Securing Mobile Devices	Randy Marchany, Virginia Tech
III.	COV ITRM Mobile Device Policy	Bob Baskette, VITA
IV.	COV ITRM SEC501-06: Important Changes	Bob Baskette, VITA
V.	Upcoming Events & Other Business	John Green, VITA
VI.	Partnership Update	Bob Baskette, VITA Michael Clark, Eric Taylor and Dean Weiner, NG

Securing Mobile Devices

"In the world of mobile, there is no anonymity" – Michael Becker

Randy Marchany
VA Tech IT Security Office and Lab
marchany@vt.edu
540-231-9523

What Were You Thinking?

- Student in my Computer Security class tried to cheat
- Duh!
- Busted!

The Things That Scare Me

- Downloading a trojan to a www site through an input screen
- Metasploit Attack – why patching systems is critical
- Bluetooth Eavesdropping
- Gigapan Inaugural Shot

The Things That Scare Me

- Data Broker Acxiom
  - InfoBase Ethnicity System
    - “Broad & precise breakdown of ethnic, religious and minority classifications
    - Matches names against housing, income, education & other demographics
- Naviant Technologies
  - Processes online product registrations for companies like IBM

Edit View History Bookmarks Tools Help

http://maps.google.com/maps?hl=en&tab=wl

Search Web | Upgrade to the latest Yahoo! Toolbar | Mail | My Yahoo! | HotJobs | Games | Music | Answers

Images **Maps** News Shopping Gmail more ▾ Sign in

Google Maps

e.g., "10 market st, san francisco" or "hotels near lax"

van nuys ca

Search Maps | Show search options

Search the map | Find businesses | Get directions

earch Results | My Maps

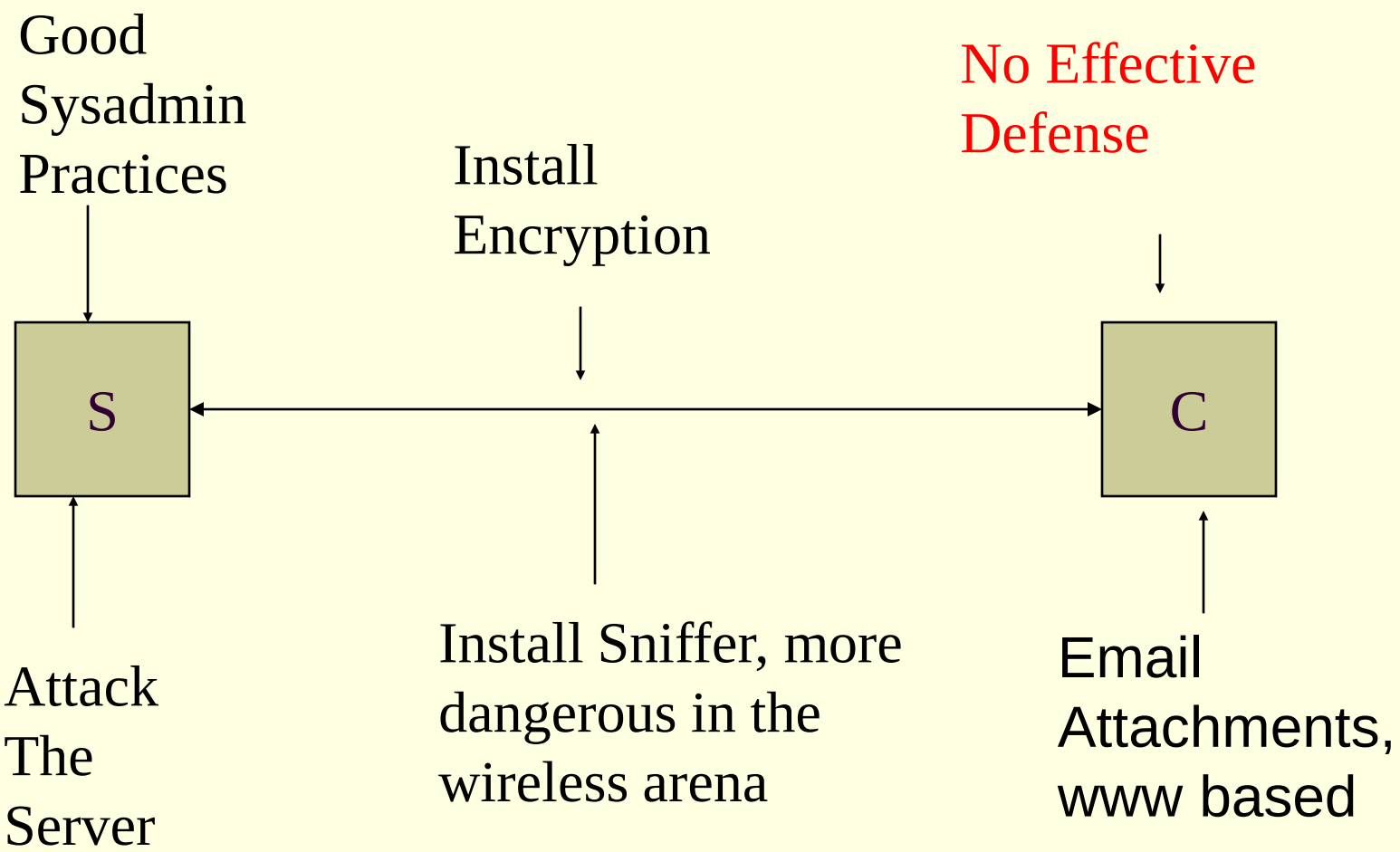
Print | Send | Link to this p

Address is approximate

Street View Help

THE THREATS

Place to Steal Personal Data



Passwords ARE the First Defense

- Bad Password Examples
- Check out http://www.skullsecurity.org/wiki/index.php/Passwords for password dictionaries
  - This is why you need to check password strength

2 Unseen
dtterm
Window Edit Options
Window Edit Options Help
locutus
My Documents
RealPlayer Basic
vncviewer
BNChange_...
unkatony
Schulz
JCSC
sans1
My Computer
Aladdin Expander 5.0
w3i2
vnc_x86_wi...
Draft_Agen...
My Network Places
Microsoft Outlook
IDandPF-Ja...
B&N - Change Managment...
assetwt
Recycle Bin
vt-probes
SANS
unit1 ir2
fsisac1
RA-Dept01-...
web2
SANS2001 Audit
SANS2001 FreewareTools
Internet Explorer
SSH Secure Shell Client
WS_FTP
vwm
EE Class
assetrisk
cacert
SANS2001 IR
03
ranum
beta
Powerpoint Presentations
FreewareTools
Acrobat Reader 4.0
Conference Papers
Netscape Communicator
Take5
VT.Site.qte
univ
uva
AOL Instant Messeng...
cc32d476
AAA
Email
CIS Rulers
Security_Ar...
Stuff
Start
Microsoft PowerPoint - [u...
1:47 PM
ame <name>] [-
vtserf.cc.vt.edu> sleep 5; xwd -out w2kvnc.xwd
100235 1 tcp 3
Apr 25
Terminal

Instant Macro-Virus Maker (IMVM) - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

The Instant Macro-Virus Maker (IMVM) v1.2

This, as far as I know, is the first (and only) on-line virus creation tool.
NO DOWNLOAD, NO WASTED TIME, NO PROGRAMING SKILL NEEDED!!!
Choose from the options (few, I know, but it's the first edition) and then copy/paste the generated code into a Word (97...2000 etc.) module named after the virus. Enjoy!!!

Virus name:

Name

Author's name:

Your name

Used macro:

AutoOpen

Text to display:

A text to show

The date when the text is shown (between 1 and 31):

00

Generate

Final source:

Document: Done

Start Insta... vtran... World'... Today... Get M... Amazi... 5:46 PM

T-Mobile said the company's computer forensics and security team were "actively investigating to determine how Ms. Hilton's information was obtained."

MSNBC

Cell phone voicemail easily hacked

They got Paris Hilton's contacts, and could get yours, too

By Bob Sullivan
Technology correspondent
MSNBC
Updated: 3:51 p.m. ET Feb. 28, 2005

"We were shocked by mobile voicemail vulnerability," he said. "This is not about (cell phone) operator bashing. This is about generating attention. They knew this and haven't generated any action."

hiltonbook.html

Edit View Favorites Tools Help
Back Search Favorites Media
http://news.bbc.co.uk/2/hi/uk_news/england/wear/3390909.stm Go

Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
England
Northern Ireland
Scotland
Wales
Politics
Education
Magazine
Business
Health
Science/Nature
Technology
Entertainment
Have Your Say
In Pictures
Week at a Glance
Country Profiles

Last Updated: Tuesday, 13 January, 2004, 10:16 GMT

E-mail this to a friend Printable version

School bans camera phones

Students at a Wearside secondary school have been banned from using mobile phones equipped with cameras, over fears images of pupils could fall into the wrong hands.

Concern grows about the possible improper use of phones

St Aidan's Roman Catholic School, in Sunderland, has banned the new generation of mobile phones, which have still and video technology.

Head teacher Tony McCourt said the move was to make the nearly 1,200 pupils at the all-boys school aware of the potential dangers.

School staff are concerned the cameras could be used to take pictures without the knowledge of youngsters, which could then be transmitted to other phones and internet sites.

The school's decision comes 24-hours after a report by children's charity NCH, which warned the new generation of mobile video phones could make the level of internet child abuse even worse.

BBC i

BBC Wear
Travel, leisure, webcams and much more from the BBC website for Wear

SEE ALSO:
- The 3G phone child abuse threat
  12 Jan 04 | Technology
- School bans camera phones
  07 Jan 04 | Essex
- Paedophile fear over phone photos
  23 Dec 03 | Scotland

RELATED INTERNET LINKS:
- Sunderland City Council
- St Aidan's RC School

The BBC is not responsible for the content of external internet sites

TOP WEAR STORIES NOW
- New inquiry over Deepcut deaths
- Man found guilty of serial rapes
- Metro strike to hit football fans
- Hat cameras to boost crime fight

Discussions Subscribe... Discussions not available on http://news.bbc.co.uk/
Internet

Your Apps Are Watching You

- Smartphones keep a lot of info about you
  - Phone numbers
  - Txt messages
  - Pics
  - Owner’s name
  - Unique ID # (can’t be disabled)
- Wall St. Journal article describes some of these “threats”

Your Apps Are Watching You

- 101 iPhone, Android apps examined
  - 56 transmitted phone's unique ID# to other companies w/o user awareness or consent
  - 47 transmitted phone's location
  - 5 sent age, gender, other personal details to outsiders
- Tracking companies are building detailed dossiers on users
- iPhone apps transmitted more data than Android apps

Your Apps Are Watching You

- Example: iPhone App TextPlus 4
  - Send phone ID # to 8 ad companies, phone's zip code, user's age, gender to 2 of them
- Pandora (iPhone, Android)
  - Send age, gender, location, phone ID# to ad networks.
- Paper Toss (iPhone, Android)
  - Send phone ID# to 5 ad companies

What’s a Phone ID?

- Unique ID number assigned to every phone
  - iPhone – Unique Device Identifier (UDID)
  - Android – various names
  - Set by phone makers, carriers or OS makers
  - Can’t be blocked or deleted
- Best tracking tool for ad companies
- Watch what you download, how often you use them, how much time you spend on them,
- Some aggregate individual data

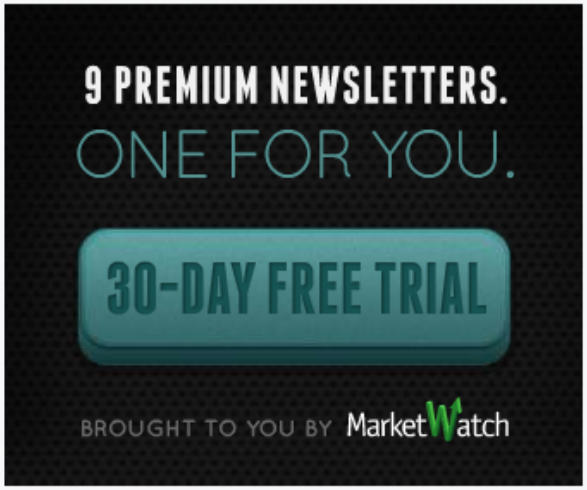
Your Apps Are Watching You

- Most apps don’t offer written privacy policies
  - 45 of the 101 apps didn’t provide privacy policies on their www site or in the app
  - Google, Apple don’t require privacy policies from app writers

iPhone | Android

Does not transmit data
Transmits data to app owner
Transmits data to third parties

App name	Username Password	Contacts	Age, Gender	Location	Phone ID	Phone number
0.03 Seconds Pro						
Age My Face						
Angry Birds						
Angry Birds Lite						
Aurora Feint II: Lite						
Barcode Scanner (BahnTech)						
Bejeweled 2						
Best Alarm Clock Free						
Bible App (LifeChurch.tv)						
Bump						
CBS News						
0.03 Seconds						
Dictionary.com						
Doodle Jump						
ESPN ScoreCenter						
Facebook						
Flashlight (John Haney Software)						
Fluent News Reader						
Foursquare						
Fox News						
Google Maps						
Grindr						
Groupon						
Hipstamatic						



Video ›

digits: Best & Worst Tech Ads in Super Bowl
5:01

digits: MySpace's Fuzzy Future
1:35

digits: Google Exec Set to be Released in Egypt
10:06

Related Stories ›

Your Apps Are Watching You

IPhone and Android apps are breaching the privacy of smartphone users, a Wall Street Journal investigation has found. 13th in a series.

Firefox Web Tool to Deter Tracking

Mozilla plans to add a do-not-track feature to its Firefox Web browser, which could let users avoid having their actions monitored online.

Smartphone Marketers Plan Privacy Rules

Facing growing public concern about privacy breaches, a

Scripts Partially Allowed, 12/13 (yahooapis.com, google-analytics.com, facebook.com, wordpress.com, chartbeat.com, fbcdn.net, wsj.net, 2mdn.net, wsj.com, facebook.net, jquery.com, doubleclick.net) | <S
46 | <OBJECT>: 0

Fluent News Reader						
Foursquare						
Fox News						
Google Maps						
Grindr						
Groupon						
Hipstamatic						
iJewels						
iLoveBeer: Zythology						
Medscape						
MyFitnessPal						
Netflix						
NYTimes						
Ninjump						
Pandora						
Paper Toss						
PerfectPhoto						
Pimple Popper Lite						
Pumpkin Maker						
RedLaser						
Ringtone Maker						
Ringtone Maker Pro						
Shazam						
Talking Tom Cat						
TextPlus 4						
The Moron Test						
The Moron Test: Section 1						
Tips & Tricks:						

Your Apps Are Watching You

IPhone and Android apps are breaching the privacy of smartphone users, a Wall Street Journal investigation ha found. 13th in a series.

Firefox Web Tool to Deter Tracking

Mozilla plans to add a do-not-track feature to its Firefox browser, which could let users avoid having their actions monitored online.

Smartphone Marketers Plan Privacy Rules

Facing growing public concern about privacy breaches, a lobby representing mobile-phone advertisers and publish called for guidelines to better protect smartphone users f intrusive tracking technologies.

The Web's New Gold Mine: Your Secrets

A Wall Street Journal investigation finds that one of the f growing businesses on the Internet is the business of sp on American consumers. First in a series.

Personal Details Exposed Via Biggest U.S. Websites

The largest U.S. websites are installing new and intrusiv consumer-tracking technologies on the computers of pe visiting their sites—in some cases, more than 100 tracki tools at a time—a Wall Street Journal investigation has f

Top Technology Stories ›

- AOL to Acquire Huffington Post
- Verizon iPhone Has New Antenna
- Google Executive Key Figure in Revolt
- Facebook Firing Case Is Settled
- Intel to Resume Shipments of Flawed Chip

Scripts Partially Allowed, 12/13 (yahooapis.com, google-analytics.com, facebook.com, wordpress.com, chartbeat.com, fbcdn.net, wsj.net, 2mdn.net, wsj.com, facebook.net, jquery.com, doubleclick
46 | <OBJECT>: 0

iPhone | **Android**

Does not transmit data
Transmits data to app owner
Transmits data to third parties

App name	Username Password	Contacts	Age, Gender	Location	Phone ID	Phone number
Advanced Task Killer						
Advanced Task Killer Pro						
Alchemy (Andrey Zaikin)						
Backgrounds (Stylem Media)						
Barcode Scanner (Zxing Team)						
Beautiful Widgets						
Bible App (LifeChurch.tv)						
Calorie Counter (FatSecret)						
CardioTrainer						
CBS News						
DailyHoroscope (Comitic)						
Dictionary.com						
ESPN ScoreCenter						
Facebook						
Fishin' 2 Go						
Foursquare						
Fox News						
Fruit Ninja						
Google Maps						
Groupon						
Handcent SMS						
Jewels						

Video ›

digits: Best & Worst Tech Ads in Super Bowl
5:01

digits: MySpace's Fuzzy Future
1:35

digits: Googl Exec Set to b Released in
10:06

Related Stories ›

Your Apps Are Watching You
IPhone and Android apps are breaching the privacy of smartphone users, a Wall Street Journal investigation ha found. 13th in a series.

Firefox Web Tool to Deter Tracking
Mozilla plans to add a do-not-track feature to its Firefox browser, which could let users avoid having their actions monitored online.

Smartphone Marketers Plan Privacy Rules
Facing growing public concern about privacy breaches, a

Scripts Partially Allowed, 12/13 (yahooapis.com, google-analytics.com, facebook.com, wordpress.com, chartbeat.com, fbcdn.net, wsj.net, 2mdn.net, wsj.com, facebook.net, jquery.com, doubleclick
46 | <OBJECT>: 0

Fishin' 2 Go						
Foursquare						
Fox News						
Fruit Ninja						
Google Maps						
Groupon						
Handcent SMS						
Jewels						
Labyrinth						
Labyrinth Lite						
LauncherPro						
Movies by Flixster						
MyBackup Pro						
MySpace Mobile						
NYTimes						
Pandora						
Paper Toss						
Ringdroid						
Robo Defense						
Robo Defense Free						
Shazam						
ShopSavvy Barcode Scanner						
Solitaire (Ken Magic)						
Talking Tom Cat						
Talking Tom Cat Free						
The Coupons App						
Toss It						
TweetCaster						

Related Stories ›

Your Apps Are Watching You
IPhone and Android apps are breaching the privacy of smartphone users, a Wall Street Journal investigation ha found. 13th in a series.

Firefox Web Tool to Deter Tracking
Mozilla plans to add a do-not-track feature to its Firefox browser, which could let users avoid having their actions monitored online.

Smartphone Marketers Plan Privacy Rules
Facing growing public concern about privacy breaches, a lobby representing mobile-phone advertisers and publish called for guidelines to better protect smartphone users f intrusive tracking technologies.

The Web's New Gold Mine: Your Secrets
A Wall Street Journal investigation finds that one of the f growing businesses on the Internet is the business of sp on American consumers. First in a series.

Personal Details Exposed Via Biggest U.S. Websites
The largest U.S. websites are installing new and intrusiv consumer-tracking technologies on the computers of pe visiting their sites—in some cases, more than 100 tracki tools at a time—a Wall Street Journal investigation has f

Top Technology Stories ›

- AOL to Acquire Huffington Post
- Verizon iPhone Has New Antenna
- Google Executive Key Figure in Revolt
- Facebook Firing Case Is Settled
- Intel to Resume Shipments of Flawed Chip

Scripts Partially Allowed, 12/13 (yahooapis.com, google-analytics.com, facebook.com, wordpress.com, chartbeat.com, fbcdn.net, wsj.net, 2mdn.net, wsj.com, facebook.net, jquery.com, doubleclick
46 | <OBJECT>: 0

Your Apps Are Watching You

- Apple Position
  - “iPhone apps cannot transmit data about a user w/o obtaining the user’s prior permission and providing the user with access to information about how and where the data will be used”
  - WSJ tests showed the apps violated this rule.
  - “Apple declines to discuss how it interprets or enforces the policy”

Your Apps Are Watching You

- Google requires Android apps to notify users what data sources the app plans to access
  - Done before the app is installed
- Possible sources
  - Phone camera
  - Memory
  - Contact list, up to 100 individual source
- Mobclix – ad exchange
  - Matches 25 ad networks with 15K apps seeking advertisers

Your Apps Are Watching You

- Ad Networks offer software kits that automatically insert ads into an app
  - Keep track where user spends time in the app
- MySpace Android App
  - Sends age, gender, device ID, to Millennial Media, an ad network
  - Millennial lists 11 types of info – age, gender, income, ethnicity, sexual orientation, political views, parental status, user income

E-Book Reading Up On You?

- E-books, Kindles, iPads, Nooks, can transmit info back to the manufacturer
  - How fast you read (turn the page)
  - Do you skip to the end? ☺
  - Where you read the book? Geolocation!
- Google Books
  - Keeps track of the last 5 pages
  - Stores more pages for “security monitoring” to prevent abusive book sharing
  - Stored for several weeks with user acct

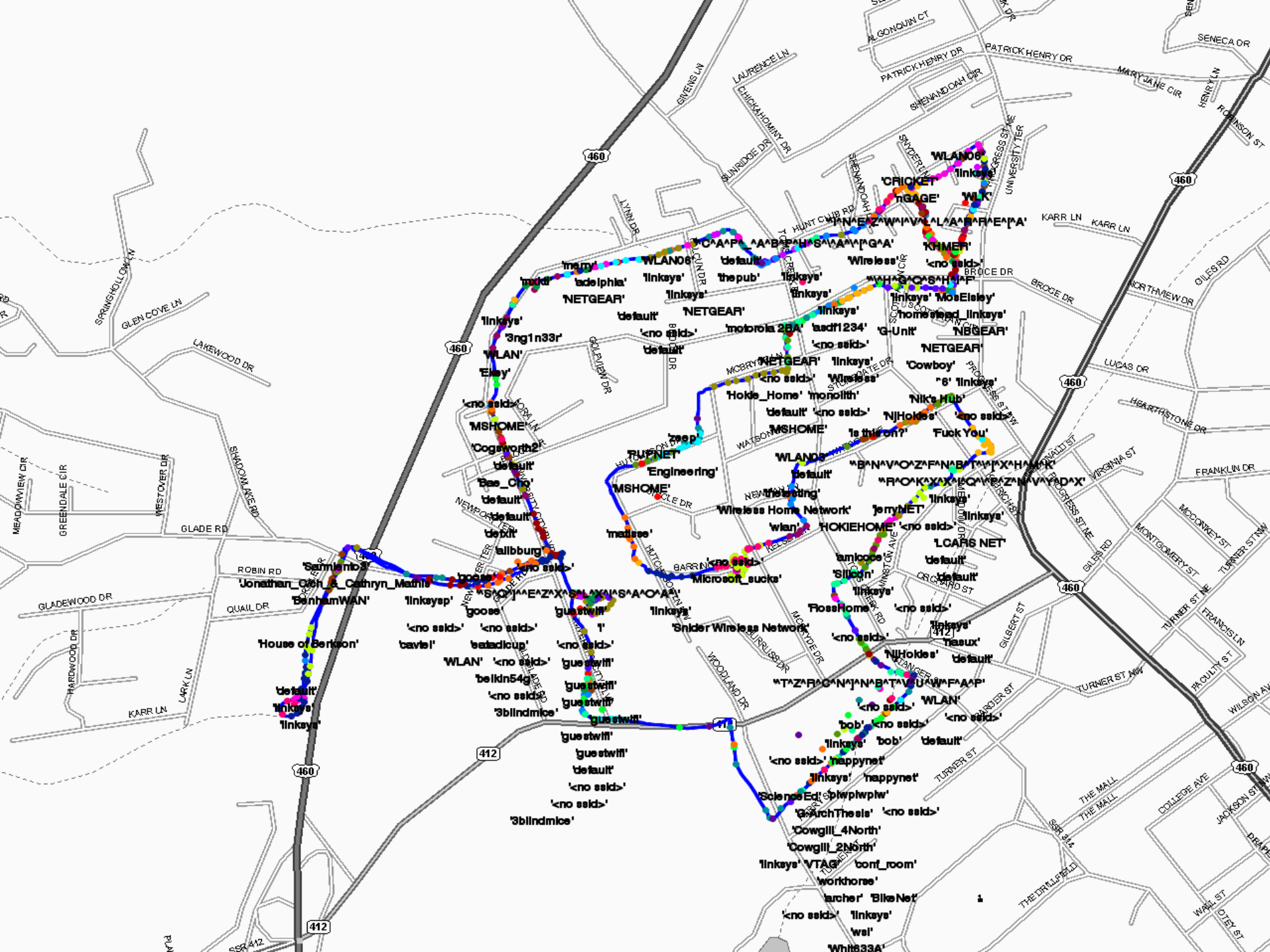
E-Books Reading Up On You?

- Apple iBook (iPad, iPhones)
  - Sends info back to Apple.
  - Only to understand customers' behavior
- FBReader
  - Free Russian reader ☺ runs on Androids.
  - Open Source
- Kindle
  - Can collect age, zip code, gender info to book authors. And those who stop on p. 45 ☺

AMBITION

THE JOURNEY OF A THOUSAND MILES SOMETIMES ENDS VERY, VERY BADLY.

www.despair.com


460
412
PATRICK HENRY DR
ALGONQUIN CT
SENECA DR
MARY JANE CIR
HENRY LN
ROBINSON ST
SHENANDOAH DR
SNYDER LN
UNIVERSITY TER
KARR LN
BROCE DR
NORTHVIEW DR
GILES RD
LUCAS DR
HEARTHSTONE DR
FRANKLIN DR
VIRGINIA ST
MONTGOMERY ST
MCDONKEY ST
TURNER ST NW
TURNER ST NE
FRANCIS LN
FACULTY ST
WILSON AVE
GILBERT ST
ORCHARD ST
PROGRESS ST NE
WALL ST
HUNT CLUB RD
LAURENCE LN
CHICKAHOMINY DR
SUNRIDGE DR
GIVENS LN
LYNN DR
GOLFVIEW DR
MCBRYDE DR
WATSON DR
NEWPORT DR
HUTCHISON DR
WOODLAND DR
MCBRUSS DR
WINSTON AVE
SPRINGHOLLOW LN
GLEN COVE LN
LAKEWOOD DR
SHADOWLAKE RD
WESTOVER DR
MEADOWVIEW CIR
GREENDALE CIR
GLADE RD
ROBIN RD
GLADEWOOD DR
QUAIL DR
HARDWOOD DR
LARK LN
THE MALL
COLLEGE AVE
JACKSON ST
THE DRILLFIELD
'WLAN06'
'linksys'
'CRICKET'
'nGAGE'
'WLK'
'KHMER'
'<no ssid>'
'Wireless'
'MosElsley'
'homestead_linksys'
'NETGEAR'
'Cowboy'
'6'
'Nik's Hub'
'NJHokies'
'Fuck You'
'mary'
'adelphia'
'thepub'
'default'
'motorola 2BA'
'asdf1234'
'G-Unit'
'3ng1n33r'
'WLAN'
'Elsey'
'MSHOME'
'Cogsworth2'
'Bas_Cho'
'Hokie_Home'
'monolith'
'zeep'
'RUPNET'
'Engineering'
'WLAN03'
'Testing'
'Wireless Home Network'
'jerryNET'
'HOKIEHOME'
'LCARS NET'
'amicoce'
'Silicon'
'RossHome'
'nasux'
'Microsoft_sucks'
'Snider Wireless Network'
'madison'
'Sammiento3'
'Jonathan_Gish_&_Cathryn_Mathis'
'BenhamWAN'
'linksysp'
'goose'
'House of Berkson'
'cavisl'
'WLAN'
'belkin54g'
'3blindmice'
'guestwifi'
'bob'
'happynet'
'ScienceEd'
'plwplwplw'
'G-ArchThesis'
'Cowgill_4North'
'Cowgill_2North'
'VTAG'
'conf_room'
'workhorse'
'archer'
'BikeNet'
'wsl'
'Whit833A'

ASK MRH - Netscape

File Edit View Go Bookmarks Tools Window Help

http://www.mrhospital.com/CustomPage.asp?guidCustomContentID=D370AF95-D801-4692-9C42-92898BDE2213

Our Network of Services | Career Center | Web Nursery | Question? Ask MRH | Find a Physician

Montgomery Regional Hospital

Your Hospital of Choice

HOME

Resources

Bill Payment

Career Center

Community Calenda

Find a Physician

Local News

Maps and Direction

Patient E-mail Servic

Phone Directory

Registration Informa

Senior Friends

Services Listing

Specialty Services

Volunteer Opportur

MRH Dining I

Room Service

Health Insura Information

Compose: (no subject)

File Edit View Insert Format Options Tools Window Help

Send Address Attach Spell Security Save

From: Gronko Scronkronk <randym@vt.edu>

To: askmrh@hcahealthcare.com

Subject:

Attachments:

Body Text | Variable Width

Unlocked Key
Mean Transmission
In the Clear!

Done

Start | ASK ... | Powe... | Micro... | Comp... | ZoneAlarm

(Untitled) - Ethereal

Follow TCP stream

Stream Content

```
220 zidane.cc.vt.edu ESMTP Mirapoint 3.4.4-GR; Wed, 3 Mar 2004 18:34:50 -0500 (EST)
EHLO vt.edu
250-zidane.cc.vt.edu Hello hc652ae72.dhcp.vt.edu [198.82.174.114], pleased to meet you
250-8BITMIME
250-SIZE 5120000
250-DSN
250-ETRN
250 HELP
MAIL FROM:<randym@vt.edu>
250 <randym@vt.edu>... Sender ok
RCPT TO:<askmrh@hcahealthcare.com>
250 <askmrh@hcahealthcare.com>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Message-ID: <40465442.7020304@vt.edu>
Date: Wed, 03 Mar 2004 16:55:14 -0500
From: Gronko Scronkronk <randym@vt.edu>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.4) Gecko/20030624 Netscape/7.1 (ax)
X-Accept-Language: en-us, en
MIME-Version: 1.0
To:  askmrh@hcahealthcare.com
Subject: senior friends information
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit

Hello. Is there a regular meeting for the Senior Friends group? If so,
when and where is it held?
Thanks. My email address is marchany@vt.edu. Please excuse the name
field of my email, I use this
mailer to communicate via mail interfaces such as yours.

thanks.

    -r.

.
250 AIQ34647 Message accepted for delivery
QUIT
221 zidane.cc.vt.edu closing connectio
```

Let Me Read Your Email!

Save As | Print | Entire conversation (1260 b | ASCII | EBCDIC | Hex Dump | C Arrays

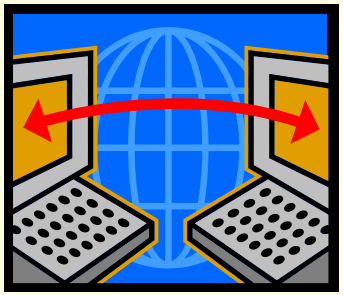
Filter out this stream | Close

Filter: (ip.addr eq 198.82.161.8 and ip.addr eq 198.82.174.114) and (tcp.port eq 25 | Expression... | Clear | Apply | File: (Untitled) 106 KB 00:03:23 | P: 336 D: 24 M: 0

Start | vtr... | Micr... | Mo... | (Un... | Foll... | ZoneAlarm | 4:57 PM

Motivation

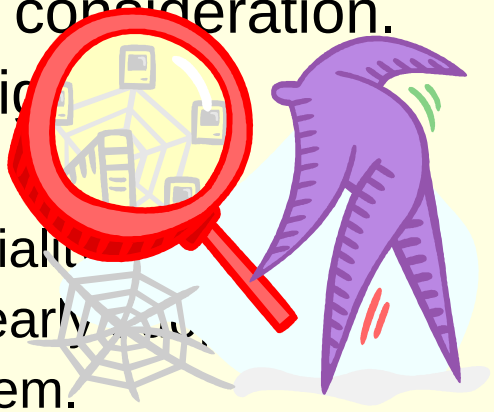
- **People want access to information all the time**
  - User expectation of information everywhere and all the time.
  - Rapid evolution to use interconnected networks.



- **Security Challenges**
  - Information sharing and security at odds.
  - Laws, regulations, and policies not keeping pace.
  - Stopgap measures.

Background for Security & Privacy

- Historically: security applied as an afterthought.
- Privacy issues receive secondary consideration.
- Not the focus of most system design.
- **Results:**
  - Loss of privacy and user confidentiality.
  - Deters knowledgeable users and early adopters.
  - Users forced to trust a flawed system.
  - Information gathering is commonplace.
- **Pervasive Goals:**
  - Mutual trust.
  - Minimally intrusive.
  - Preserve invisibility.



Tradeoff between exploiting benefits of shared information and giving away one's personal privacy.

Security Best Practices

- **PDAs, smart phones, RFID tags, and WSN.**
- **Device size decreases and mobility increases.**
- **Balance confidentiality, integrity, and availability.**
  - Device constrai[illegible]ecurity capabilities.
  - [illegible]ense.

Traditional
- Firewall
- IDS
- ADS
- Antivirus
- Encryption

Transitional
- Hybrid IDS
- Reputation & Trust

Future
- Secure Design
- Pervasive Data
- User Confidentiality
- Filtered User Data

Technical Solutions for Protection Privacy

- **Privacy policy encoding.**
  - Privacy profile is based on user's willingness to share information.
  - System compares user's profile with w
    policy.

- **Anonymization tools.**
  - Abound on the Internet today.
  - Transitioning to pervasive environments.
  - Deter unwanted information collection.
- **Hippocratic databases.**
  - Enforce privacy policy, explicit access checks.
  - Users "opt-in" or "opt-out".

Technical Solutions for Protection Privacy

- **Privacy preserving data mining.**
  - Allows businesses to derive aggregated client data for insight.
  - Maintains user privacy.
  - Discards personal information.
- **Information sharing across private repositories.**
  - Users will disclose data, but do not want it collected in dossiers.
  - Data retrieval from disparate storage.
  - Multiparty data sharing framework needed.

Privacy & Legal Concerns with Technologies

- **Location-aware.**
  - ***E911 enabled smart phones*** offer 300 meter accuracy.
  - ***Placelab*** (GSM, WiFi, & GPS) gives 300 to 10 meter accuracy.
  - Limited governance, laws, regulations, and policies.

RFID Technology

- **RFID tags.**
  - first “true” pervasive technology.
  - Correlation tracking for inventory mgt
  - Potential misuse by combining user habits with tags tracking data

Table 1. RFID tag characteristics comparison.

Tag Type	Memory	Reprogrammable	Processor	Power Source	Range	Reusable
Passive	ROM	No	No	RF	**2 Meters**	No
Active	RAM / ROM	Yes	8-bit	Battery	**1 Kilometer**	Yes
Hybrid	ROM	Yes / No	No	Battery	**20 Meters**	Yes

Privacy & Legal Concerns with Technologies

- **Where do we draw the line?**
  - Limits must be set.
  - Laws, court rulings, and public opinion will draw the line.

Limits must be set with pervasive technology, … else these systems will offer no privacy anywhere.

Dr. Pottie, UCLA

The *goal of hearings* is not to create legislation that says the technology could never be used, but it is to gain a better understanding of the impacts.

Senator Bowen

Threat Summary

- Data Disclosure
- Data Modification
- Denial of Service Attacks
  - Drain the battery

MOBILE DEVICE FORENSICS

Device Information

Oxygen Forensic Suite 2010 Analyst

Device View Tools Service Help

Desktop Disconnect Search Export Print Help

Device Info

Device photo

Device details

Crime scene: Central Park

Device Info
Phonebook
Calendar
Tasks
Messages
Event Log
File Browser
Extras

New device (N73-1)

Close device

Attribute name	Attribute value
Common Info	
Alias	New device (N73-1)
Retail Name	Nokia N73-1
Manufacturer	Nokia
Internal Name	RM-133
IMEI	356425024880535
Hardware Revision	N/A
Software Revision	V 4.0735.3.0.2 (01-09-2007)
Flight Mode	No
Extracted by version	2.7.0.232
Extraction Time	03.06.2010 13:18:14
Network Info	
Operator	Beeline
Network	BEELINE
Network Mode	2
Network Status	2
Network Band Info	0
Network Access	0
MCC	250
MNC	99
Cell ID	13862
LAC	5407
Device owner numbers	
Phone	9843908745
Work	987298754
Cellular	87987555
Car phone	999834278
Case attributes	
Owner	Robert Dobbs
Inspector	Inspector
Case	887341764
Evidence number	76548647

Section	Statistic
Phonebook	25
Contacts	25
Caller groups	6
Speed dials	8
Calendar	29
Meeting	17
Memo	5
Anniversary	7
Tasks	15
Completed	3
Outdated	11
Incompleted	1
Messages	189
Incoming Messages	128
Outgoing Messages	18
Sent Messages	42
Sent failed Messages	1
Event Log	105
Dialed calls	26
Answered calls	4
Missed calls	7
SMS	30
Packet	38
File Browser	1900
Images	254
Documents	21
Applications	4
Database files	10
Melodies	14
Videos	6
Other files	1591

Add photo Remove photo Set default photo Download image

n73_2 Nokia N73-1

Analyst version: 2.8.0.534 Expires in 874 days Extraction Time: 03.06.2010 13:18:14

Data Search

Oxygen Forensic Suite 2010 Analyst

Device View Tools Service Help

Device Info | Backup Extraction Wizard | Tutorial | Help | Quick filter:

Desktop | New device (N73-1) | New device (iPhone 3G)

Desktop

Common tasks

Connect new device

Change a database storage place

Devices | Search data

Search only: Any text | Contact

Location: Open devices

Text: +79

For example, JohnDoe@gmail.com

Case sensitive

Find Now | Stop | New Search

History | Save | Rename | Delete | Export | Print

Search result

+79 (02.08.2010 10:

Type	Name	Description	Device
	Espozito Dan Sr.	Private: +79060355896	New device (N73-1
	Mr. Wilkinson Paul	Orders: +79630411041	New device (N73-1
	Johnes Alex Sr.	Mobile (partners): +796...	New device (N73-1
	Collingwood Andrew	Mobile: +79060355963	New device (N73-1
	Beards Michael	Zade Ahmed: +7963604...	New device (N73-1
	Cook John	Mobile: +79035841186	New device (N73-1
	Rosen Jane	Mobile: +79636041041	New device (N73-1
	Davidson Ivan	Shop: +79060355934	New device (N73-1
	Karmanlis Basilidis	Paul Williams: +7967024...	New device (N73-1
	James Simon	Mobile: +79647910398	New device (N73-1
	Bobson Nick	Mobile: +79647910284	New device (N73-1
	+79035841186	Remote party: +790358...	New device (N73-1
	+79035841186	Remote party: +790358...	New device (N73-1

Object Details:

Contact

Mr. Wilkinson Paul
Cantine: "Three sharks" restaurant
Cook: Chef
Parties: +489562258423
Orders: +79630411041
Contracts:
paul_wilkinson@usarestaurants.us
Web address:
http://www.3sharks.us/aboutus/chef
Impressions:
Really delicious! I should recommend this restaurant to my Boss.
Country/Region: Anvilania
Postal/ZIP code: 2937123
State/Province: District 42
City: Stem city
Street: Green Street, 78
P.O. Box: P.O. 37

Analyst version: 2.8.0.531 | Expires in 874 days | Total devices: 30, open: 2, filtred: 30

Data Search

Oxygen Forensic Suite 2010 Analyst

Device View Tools Service Help

Device Info | Backup Extraction Wizard | Tutorial | Help | Quick filter:

Desktop | New device (G1) | New device (iPhone 3GS) | New device (iPhone 3GS)

Desktop

Common tasks

Connect new device

Change a database storage place

Devices | Search data

Search only: Any text | Contact

Location: Open devices

First Name: Andrew

Last Name:

Phone numbers:

Other fileds:

Case sensitive

Include contacts activities

Find Now | Stop | New Search

History | Save | Rename | Delete | Export | Print

Search result

Andrew (29.07.2010

Type	Name	Description	Device
	Collingwood Andrew	Name: Collingwood Andrew	iTunes Backup (5
	+79060355963	Number: +790603... Remote party: +790603...	iTunes Backup (5
	+79060355963	Number: +790603... Remote party: +790603...	iTunes Backup (5
	jasonp45	Mobile number: +790603...	iTunes Backup (5
	Collingwood Andrew	Name: Collingwood Andrew	New device (N95
	+79060355963	Number: +790603... Remote party: +790603...	New device (N95
	+79060355963	Number: +790603... Remote party: +790603...	New device (N95
	+79060355963	Number: +790603... Remote party: +790603...	New device (N95
	+79060355963	Number: +790603... Remote party: +790603...	New device (N95
	Collingwood Andrew	Remote party: Collingwo...	New device (N95
	Collingwood Andrew	Remote party: Collingwo...	New device (N95
	+79060355963	Number: +790603... Remote party: +790603...	New device (N95

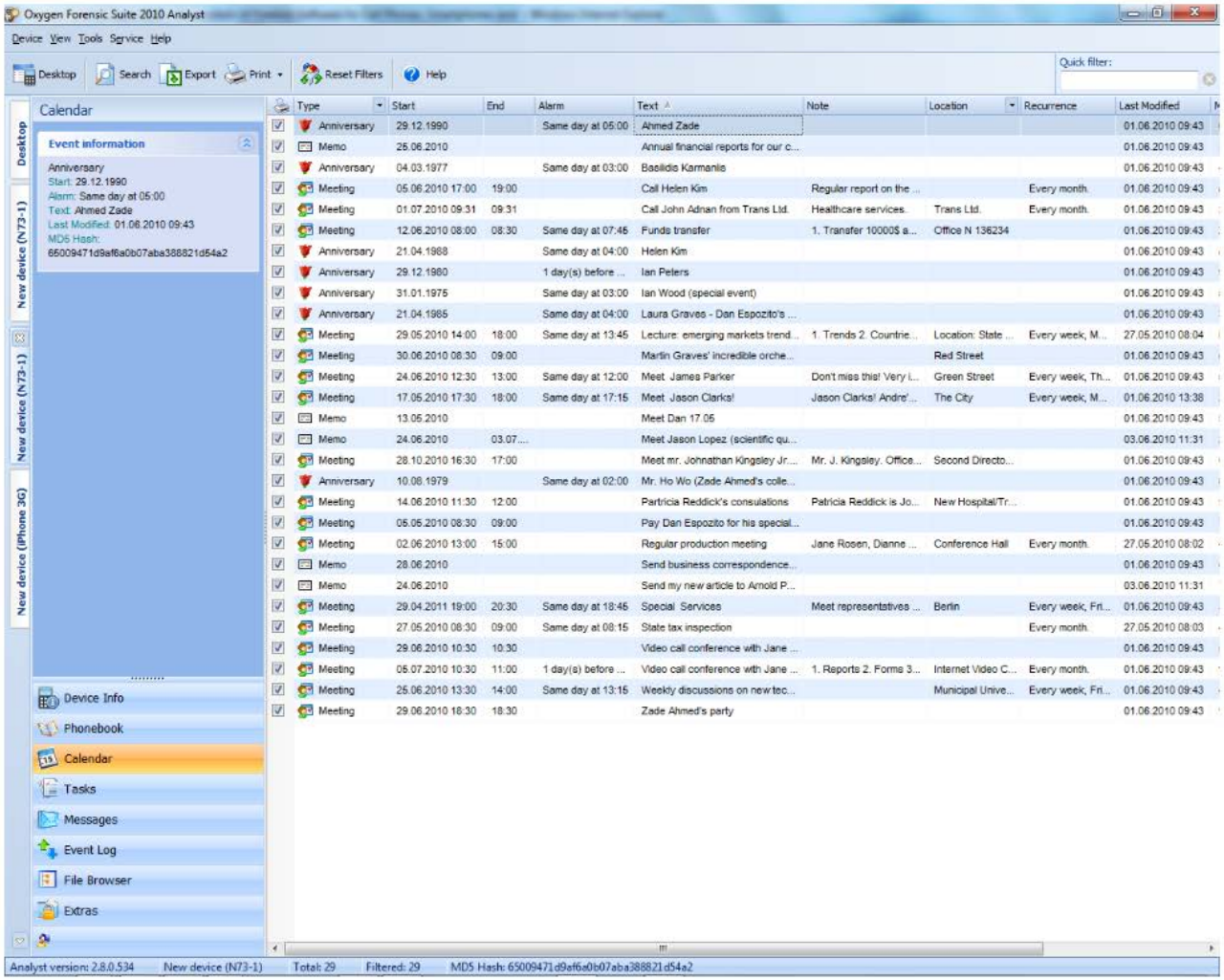
Object Details:

Contact

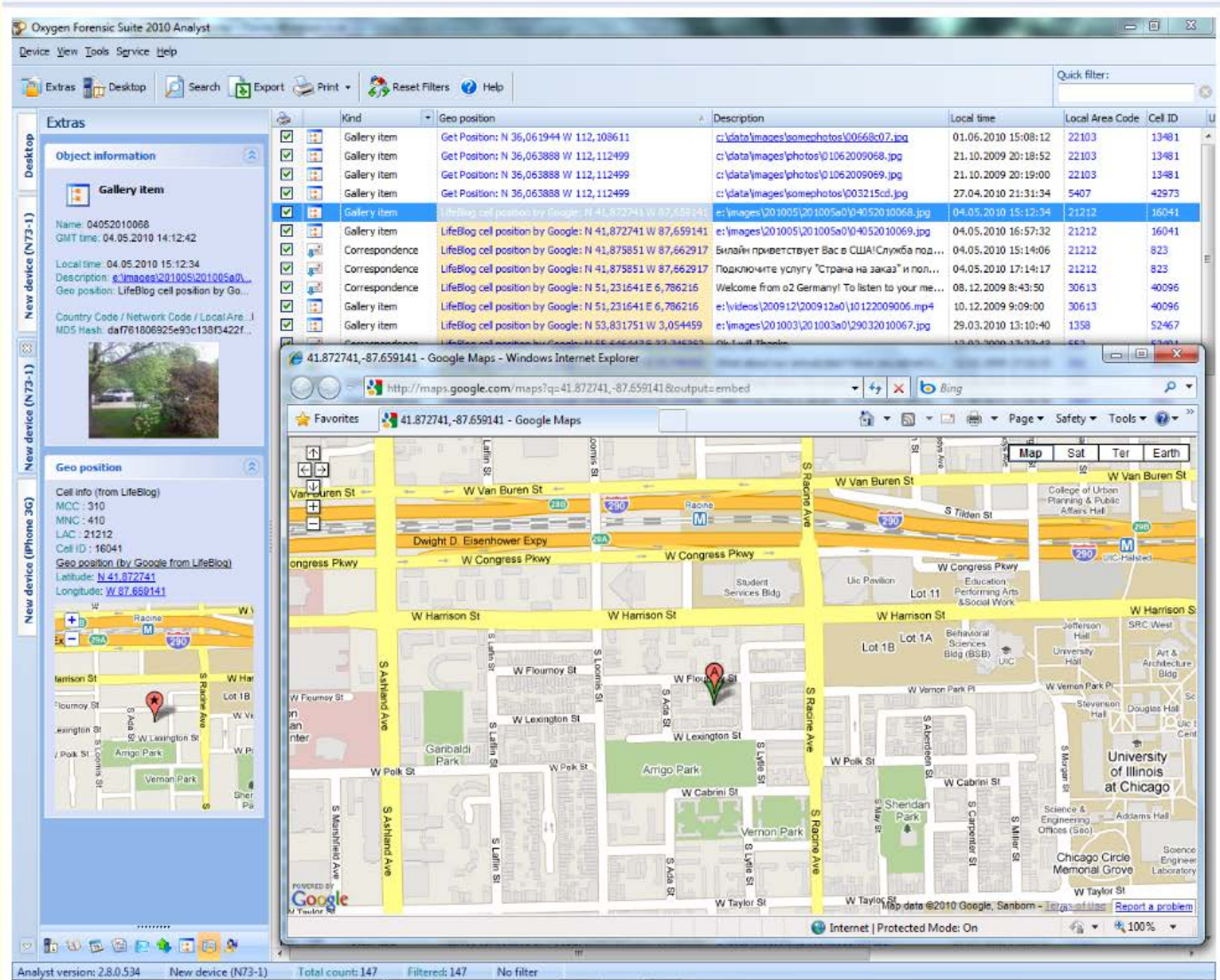
Collingwood Andrew
Birthday: 11.02.1949
Company: Private services
Job title: Specialist
Tel. (business): 1625930
Tel. (home): 987329487324
Tel. (business): +9611827360
Mobile: +44125369442
Mobile: +79060355963
Fax (business): 2343242
E-mail (home): andrew.collingwood.73@gmail.com
E-mail: ajcollingwood@hotmail.com
Note:
Illegal recycling ,utilization. Industrial wastes...?
Video call: 456434
Country/Region: Ethniklashistan
State/Province: Second District
City: New City
Street: Dandellion st.
Caller group: Distributors

Analyst version: 2.8.0.494 | Expires in 878 days | Total devices: 27, open: 26, filtred: 27

Calendar & tasks



geopositioning



Web cache

Oxygen Forensic Suite 2010 Analyst

Device View Tools Service Help

Extras Desktop Search Export Print Filters Views Sort Help

Quick filter:

Desktop | New device (N73-1) | New device (N73-1) | New device (iPhone 3G)

Extras

Tasks for selected objects

Save to ...

Show properties

Proceed to

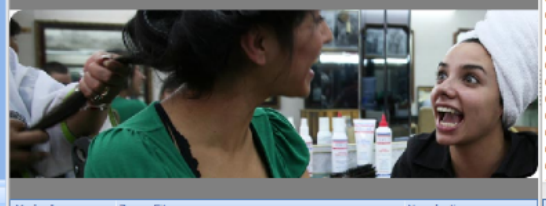
Back to Extras

Object information

Name: image_6.jpg
Type: JPG File
Size: 27,05 KB
Path: C:\cache\
Modified: 21.05.2009 16:16:14
MD5 Hash:
2de1b50df80a0ccf2b5735126b5e783a
Url: http://www.nokia.com/NOKIA_COM_1/f

Web cache | Web bookmarks | Web history

Name	Path	URL	Type	Size	Date modified	Filter	MD5 Hash
JPG FILE							
convergence_background_...	C:\cache\	http://europe.nokia.com/PRODUCT...	JPG File	23,35 KB	21.05.2009 16:27:24	Images	15ebb9e4364535fbe37705224..
image_6.jpg	C:\cache\	http://www.nokia.com/NOKIA_CO...	JPG File	27,05 KB	21.05.2009 16:16:14	Images	2de1b50df80a0ccf2b5735126b..
intro_background.jpg	C:\cache\	http://www.nokia.com/NOKIA_CO...	JPG File	13,24 KB	21.05.2009 16:16:12	Images	ec3df1cd290d12f8cf8e988e66..
HTML DOCUMENT							
633408995949512 50index....	C:\cache\	http://wap.beeline.ru/	HTML Docum...	198 B	28.02.2007 6:19:54	Documents	aed083ac460df96de0484087a..
633408996208577 50index....	C:\cache\	http://palm.newsru.com/	HTML Docum...	7,89 KB	28.02.2007 6:20:22	Documents	77988a7e0ac34c9d3c4b417b7..
633408997957630 00index....	C:\cache\	http://www.google.ru/	HTML Docum...	1,97 KB	28.02.2007 6:23:16	Documents	9f8c2aceccd51a040f9859c9e8..
634109308356387 50index....	C:\cache\	http://avatars.yandex.net/get-av...	HTML Docum...	3,84 KB	18.05.2009 15:27:16	Documents	4ee6f06343cd12370f2e625ff7..
634111936022640 00index....	C:\cache\	http://europe.nokia.com/nseries/	HTML Docum...	20,04 KB	21.05.2009 16:26:42	Documents	7d293b5e4d06838e27e24f91a..
634354377122287 50index....	C:\cache\	http://oxygen-forensic.com/en/	HTML Docum...	26,96 KB	26.02.2010 10:55:14	Documents	51b324f67d2c66adabb3d46b0..
index.html	C:\cache\	http://img5-fotki.yandex.ru/getx/1...	HTML Docum...	2,07 KB	28.02.2007 6:22:52	Documents	544cae8c184faf11a9953109d2..
HPS FILE							
entrylist.hps	C:\cache\		HPS File	0 B	05.12.2008 15:03:22	Other files	d1f3bcc50557b072da002a27f9..
GIF IMAGE							
1px.gif	C:\cache\	http://oxygen-forensic.com/images...	GIF image	43 B	26.02.2010 10:55:44	Images	6199e85c77a674344a8a46f1f8.
breadcrumb_icon.gif	C:\cache\	http://europe.nokia.com/pics/brea...	GIF image	280 B	21.05.2009 16:27:20	Images	6fe9a909ebb8057106a79c770f.
btn_go2_1b.gif	C:\cache\	http://europe.nokia.com/res/sitese...	GIF image	1,41 KB	21.05.2009 16:27:20	Images	c0026ad4966d436ce5a72b2a7..
c.gif	C:\cache\		GIF image	0 B	26.02.2010 10:53:42	Images	ed1b676bb368f722a27627f17...
clear.gif	C:\cache\	http://i.msdn.microsoft.com/Global...	GIF image	85 B	26.02.2010 12:00:42	Images	a8d0f47d627e5cb22a6694a8e..
CN.gif	C:\cache\	http://oxygen-forensic.com/images...	GIF image	121 B	26.02.2010 10:55:20	Images	4fa7d7e3f29ae188cb163243dd.
D_D_Redbooks_Feb10.gif	C:\cache\		GIF image	7,08 KB	26.02.2010 10:53:54	Images	390a934639effbe3e46ba4dd1...
hp-oj-bullet.gif	C:\cache\		GIF image	0 B	26.02.2010 10:54:02	Images	8f37645b3310458ee894f8ccab..
hp-task-bg.gif	C:\cache\		GIF image	0 B	26.02.2010 10:54:00	Images	4f385aad8bc4e32929c26be69...
hp-task-columns-bg.gif	C:\cache\		GIF image	0 B	26.02.2010 10:54:02	Images	5e3c5547985dbb9fd181af18ae.
hp-task-end.gif	C:\cache\		GIF image	0 B	26.02.2010 10:54:02	Images	c61047d70fbeeb2d75e0df2ca9..
hotab-next-six-tabs.gif	C:\cache\		GIF image	0 B	26.02.2010 10:54:00	Images	6d47e64bd10dce669ba406154..



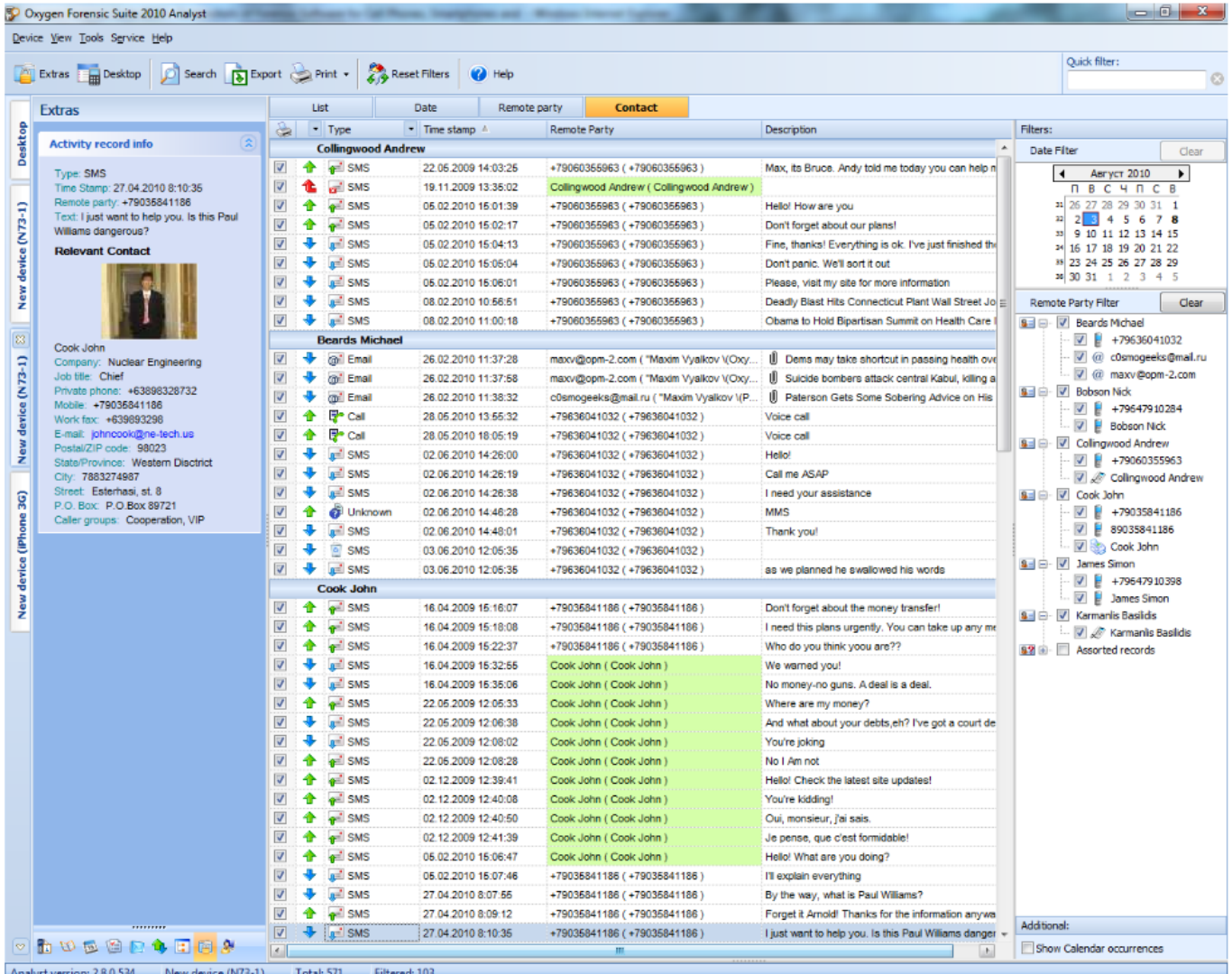
```
00000000: FF D8 FF E0 00 10 4A 46  49 46 00 01 02 00 00 64
00000010: 00 64 00 00 FF EC 00 11  44 75 63 6B 79 00 01 00
00000020: 04 00 00 00 32 00 00 FF  EE 00 0E 41 64 6F 62 65
00000030: 00 64 C0 00 00 00 01 FF  DB 00 84 00 08 06 06 06
00000040: 06 06 08 06 06 08 0C 08  07 08 0C 0E 0A 08 08 0A
00000050: 0E 10 0D 0D 0E 0D 0D 10  11 0C 0E 0D 0D 0E 0C 11
00000060: 0F 12 13 14 13 12 0F 18  18 1A 1A 18 18 23 22 22
00000070: 22 23 27 27 27 27 27 27  27 27 27 27 01 09 08 08
00000080: 09 0A 09 0B 09 09 0B 0E  0B 0D 0B 0E 11 0E 0E 0E
00000090: 0E 11 13 0D 0D 0E 0D 0D  13 18 11 0F 0F 0F 0F 11
000000A0: 18 16 17 14 14 14 17 16  1A 1A 18 18 1A 1A 21 21
```

Mode: Image | Zoom: Fit | No selection

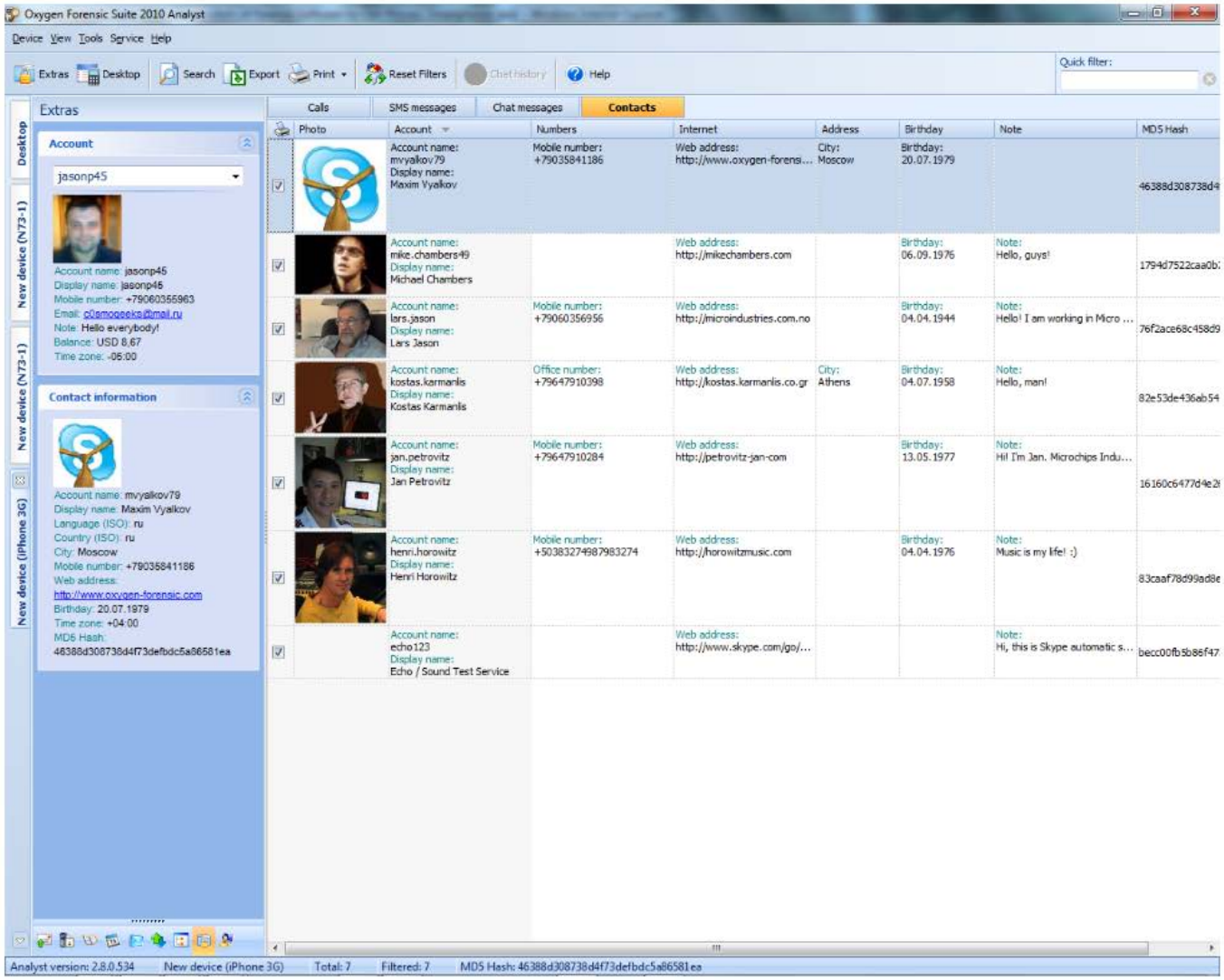
Mode: Hex | Encoding: ANSI (Windows) | No selection

Analyst version: 2.8.0.534 | New device (N73-1) | Total:191 objects (27,05 KB) | Selected: image_6.jpg | MD5 Hash: 2de1b50df80a0ccf2b5735126b5e783a

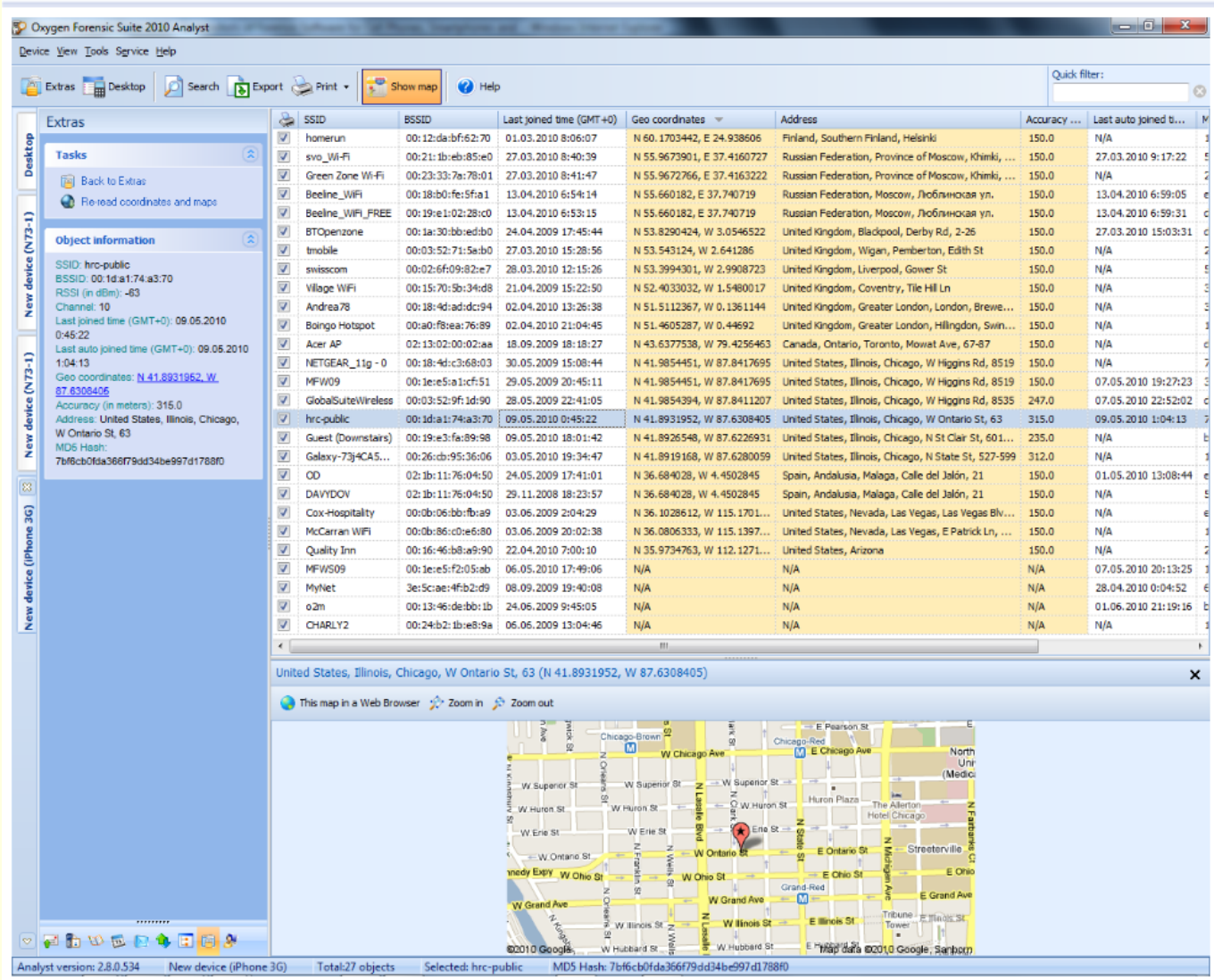
Phone history



Skype analyzer



Wifi analyzer



Calendar & Tasks

	A	B	C	D	E	F	G	H	I	J	K	L
1	**Subject**	**Location**	**Note**	**Number**	**Start date/time**	**End date/time**	**All day**	**Type**	**Alarm**	**Recurrence**	**Last m**	**SHA-2 Hash**
2	Jessica Simpson				04.02.2008 12:00	04.02.2008 15:00	False	Meeting	Alarm type: Loud	Repeat forever	N/A	1ebc0b8a5ce90d9fedbf2c6d
3	Mr Collins				05.02.2008 10:00	05.02.2008 12:00	False	Meeting		Repeat forever	N/A	e2b30d86602da20955c86ae
4	Meet with Diana	Cafe			06.02.2008 07:00	06.02.2008 09:00	False	Meeting		Repeat forever	N/A	e372f2c05560b56f4102d872
5	Mr Thomson	Bank			07.02.2008 09:00	07.02.2008 12:00	False	Meeting	Alarm type: Loud	Recurrence: monthl	N/A	fc5f898c195bfe40f4a20ab0c
6	Mr Simons	Bank			08.02.2008 12:00	08.02.2008 13:00	False	Meeting		Repeat forever	N/A	9f05fda8036e5eadeb9a315d
7	Peter Samon	Restaurant			09.02.2008 15:00	09.02.2008 17:00	False	Meeting		Repeat forever	N/A	4e31b397056d52d376daa20
8	Visit my father				10.02.2008 13:00	10.02.2008 15:00	False	Meeting	Alarm type: Loud	Repeat forever	N/A	9709ea0d59301bbd133a986
9	Sara O'Connor	Office			11.02.2008 09:00	11.02.2008 10:00	False	Meeting	Alarm type: Loud	Repeat forever	N/A	035dc0469176fd1bb7841ecc
10	Mr Thomson	Bank			12.02.2008 08:00	12.02.2008 09:00	False	Meeting	Alarm type: Loud	Repeat forever	N/A	c80edbb882eed8651f74267
11	ytfyfyfyffy				14.02.2008 09:44	14.02.2008 10:44	False	Meeting		Repeat forever	N/A	d536d8c3e494b142507e84f
12	Patrick			0989787876	04.02.2008 09:00	04.02.2008 09:00	False	Call		Repeat forever	N/A	18c7e0101347ec0d576042a
13	Sara			64545454	05.02.2008 15:00	05.02.2008 15:00	False	Call	Alarm type: Loud	Repeat forever	N/A	a5edc20a915a25505798e2f
14	My birthday				04.02.2008	04.02.2008	True	Birthday		Recurrence: yearly	N/A	61bbc891ad3a5cb913aa343
15	Carol's birthday				07.02.2008	07.02.2008	True	Birthday	Alarm type: Loud	Recurrence: yearly	N/A	5a502167aa9d269cd5d8b8a
16	Mother's birthday				07.02.2008	07.02.2008	True	Birthday	Alarm type: Loud	Recurrence: yearly	N/A	a039f3dc2e41d4030912e283
17	Mike's birthday				09.02.2008	09.02.2008	True	Birthday	Alarm type: Loud	Recurrence: yearly	N/A	38f483750f7dec7191c53c1c
18	Jessica Right				12.02.2008	12.02.2008	True	Birthday		Recurrence: yearly	N/A	0a91ed4a2256070f3eee63c1
19	To get photos				06.02.2008	06.02.2008	True	Memo	Alarm type: Loud	Recurrence: monthl	N/A	e9d01b82621903826134963
20	To renew my OxyCube license				10.02.2008	10.02.2008	True	Memo	Alarm type: Loud	Repeat forever	N/A	c685d8af3db39005677d072
21	To go to the laundry				11.02.2008	11.02.2008	True	Memo		Repeat forever	N/A	73f0352cdf43de40947eea8a
22	Doctor				12.02.2008	12.02.2008	True	Memo		Repeat forever	N/A	0767d6afdbdf735da8db7144
23	To place the order with OOO Soft				05.02.2008	05.02.2008	True	Reminder	Alarm type: Loud	Repeat forever	N/A	0acf66d56f4bdeb7d627a6a5
24	To water mother's folwers				08.02.2008	08.02.2008	True	Reminder	Alarm type: Loud	Repeat forever	N/A	bac73e0dda72dcf6edfb44f4f
25	To call Sara				08.02.2008	08.02.2008	True	Reminder	Alarm type: Loud	Repeat forever	N/A	0e31c5c4276202e0ae6eb42
26	To call Mrs Brown about the baby				10.02.2008	10.02.2008	True	Reminder	Alarm type: Loud	Repeat forever	N/A	8cb67b27a810aa83e70c11e
27												
28												

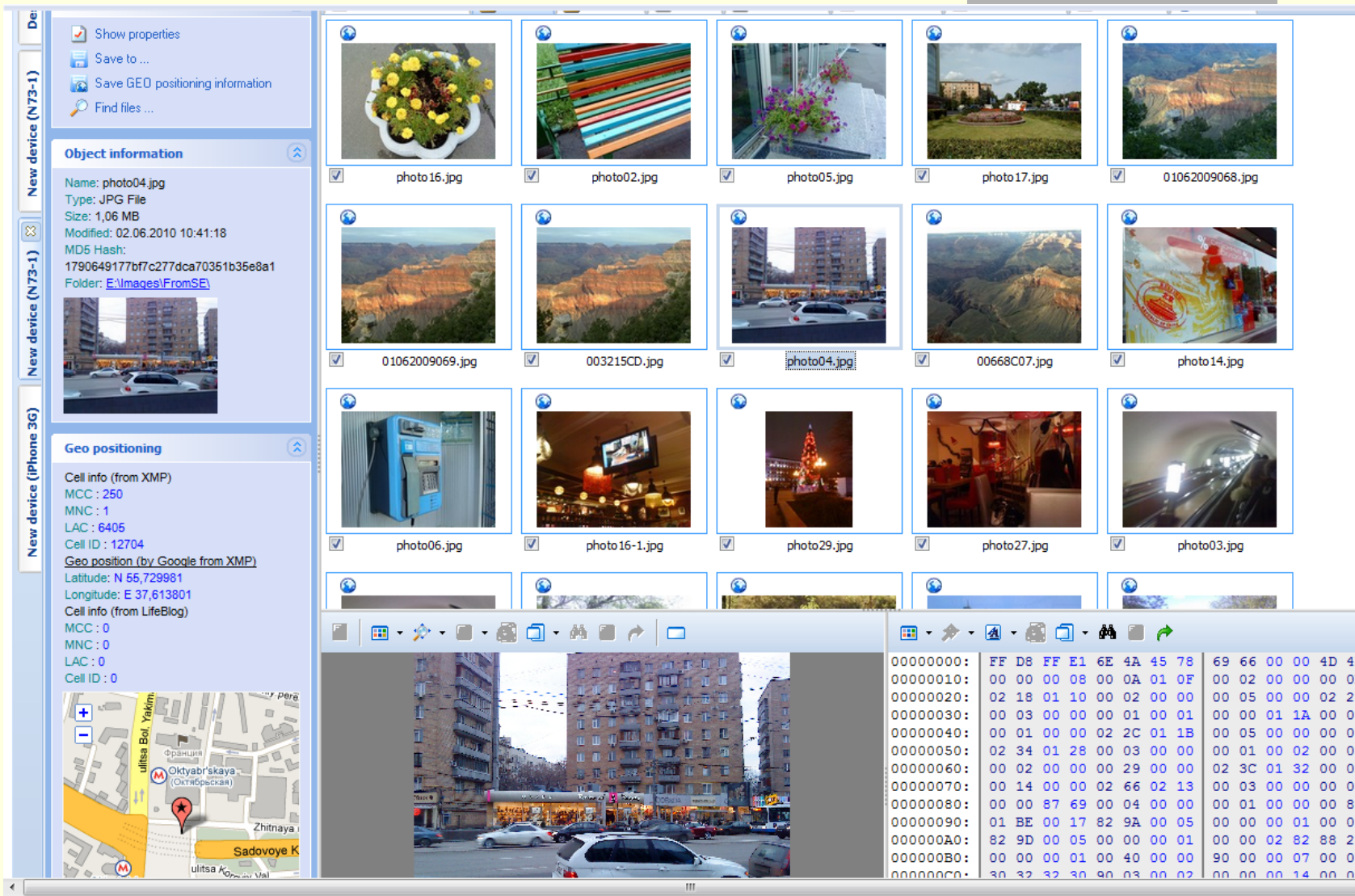
Tasks

Tasks

Oxygen Forensic Suite 2 - 2.1.0.15

Priority	Time stamp	Description	Last modified date	MD5 Hash
Low	Due time:03.03.2009 00:00:00 Done time:02.03.2009 00:00:00	C	02.03.2009 18:30:08	e9671e80831670ad968a9e4e002e981c
High	Due time:03.03.2009 00:00:00 Alarm:Same day at 19:00	Dentist	03.03.2009 11:57:41	cf354efe5373eace3521f89b9eb5bce3
Normal	Due time:12.03.2009 00:00:00	Water flowers	03.03.2009 11:58:56	2d94aeb67a95dee2b9695fab45c6d921
Normal	Due time:07.03.2009 00:00:00 Alarm:Same day at 11:00	Meet Ann	03.03.2009 11:59:37	3ce6402f2bf3a19779393e4dd16c9733
Normal	Due time:07.03.2009 00:00:00	Order OxyCube	03.03.2009 12:00:27	c9b1436cfad9e73b83ad6ee828d8b189
Low	Due time:07.03.2009 00:00:00 Alarm:Same day at 08:00	Buy medicine	03.03.2009 12:01:18	e9cb3f5d0bc7532498a9eeea322fa55a
High	Due time:05.03.2009 00:00:00	meet Don Pedro	03.03.2009 12:02:18	c12afbf8264d31caeb9d5f9c5f0b8589
High	Due time:06.03.2009 00:00:00 Alarm:Same day at 08:00	Money from Kate	03.03.2009 12:03:05	0f2d33e46b9f23ae3497c51c5be11912

filebrowser



File Manager

File manager

Oxygen Forensic Suite 2 - 1.4.0.21

	File name	Size (bytes)	Time stamp	MD5 Hash
C:\				315F3EADA434C4AEF04F48BA7337F417
	FIM_fixed_id	01.01.2007 9:03:06	8	382650D6D98E0661570E9F98220D27FE
	FIM_perm_id	19.11.2008 11:51:48	19608	FE67D294C090DEAC20ADE0AD49D59A13
	FIM_punique_id	19.11.2008 11:51:48	6216	C9A51B49225C723A7A51FC5EB19807CD
	test.docx	30.10.2008 12:55:18	9984	4DAD6C552CB3E01CF61B6E4A055D0918
C:\HTTP\				B878916324B26CF0B66FEFBFE03EC6C0
	проверка чтения файлов	28.01.2007 4:44:50	86	579298E7EA94949326768EB7AA30FED7
C:\HTTP\cache\				D311E02B7187BD7626A16309DB6D298E
	C4O0dapkrDDvQ8ChC.dat	16.05.2008 16:20:36	4296	50D7EFBA115D4698D483BA9CBA09EEC8
	C4O0dapkrDDvQ8ChC.hdr	16.05.2008 16:20:36	441	A349BC44FE7CE4F3120E7EC3254966FB
	C59TFXVcPqijYJ12k.dat	16.05.2008 16:20:34	851	F213CE7CE85904556AB5956547768FD4
	C59TFXVcPqijYJ12k.hdr	16.05.2008 16:20:34	366	B75AF7D3B0A6705A12C7358C5D95F2CD
	CAadrl1IMSaZtlup3.dat	16.05.2008 16:20:34	595	D33E8CB3A4BCFB5DC8A556B33EBB375D
	CAadrl1IMSaZtlup3.hdr	16.05.2008 16:20:34	366	ACFF506BD132D66255D303A39C08FEA9
	Cc8OycMaRUY5SvB2t.dat	16.05.2008 16:20:34	1030	332EC7004B43C66675DE44B167D3DD2E
	Cc8OycMaRUY5SvB2t.hdr	16.05.2008 16:20:34	335	D062649C67DAF0FF1EEA1E195FED302E
	CGFwk3QH9IMq5s28J.dat	16.05.2008 16:20:34	1413	02E3ADEED36EDC90F493FEE19C3D2EBA
	CGFwk3QH9IMq5s28J.hdr	16.05.2008 16:20:34	335	AD09ECCE75F5CBE0BCA5AC6C487F702D
	CH8qKaozjsHfkY8n4.dat	16.05.2008 16:20:34	906	1DB8850C930637C1B5E527B7071BEEE2
	CH8qKaozjsHfkY8n4.hdr	16.05.2008 16:20:34	366	F0C62303EB7421CC1DCE3B147AE4BA6E
	CmL7oJFLuxDgofGdu.dat	16.05.2008 16:20:34	1581	E2B5EE552ACA8E99D6FEC32C47521AD9
	CmL7oJFLuxDgofGdu.hdr	16.05.2008 16:20:34	336	065BF01870E13DCFBDF9D8E785601526
	CNmjQf2BAAtMCjhPR.dat	16.05.2008 16:20:34	1011	923A42F97497A3E70099ADC5E96FDBEB
	CNmjQf2BAAtMCjhPR.hdr	16.05.2008 16:20:34	335	504E0C7A4DF24AC58875BF5AE0AB35D8
	CP2GeqOiaXabxFCRL.dat	16.05.2008 16:20:36	5	663ABB2790B1824723FEC4A0DE3D70DF
	CP2GeqOiaXabxFCRL.hdr	16.05.2008 16:20:36	941	A2D72AFBE1597B9C2C08D09F956B1324
	CrBaYFi67JvMFgvby.dat	16.05.2008 16:20:34	1568	560ACA1DE058F9530AD4209C70B92AB9
	CrBaYFi67JvMFgvby.hdr	16.05.2008 16:20:34	553	2E992A294AEBA2D601EB81FE2C7C2DC2
	CTtEK7OF0eNzsv3RS.dat	16.05.2008 16:20:32	670	E2541C3372CEABD15B07F782931347D8
	CTtEK7OF0eNzsv3RS.hdr	16.05.2008 16:20:32	434	74EFD7F76974E7578C9DA29E451FC356
	CuGDTdfhCttaRl1C8.dat	16.05.2008 16:20:32	7852	5D0BCF25B6E45E8508E50C3A87B483EC
	CuGDTdfhCttaRl1C8.hdr	16.05.2008 16:20:32	348	DC6A3E2CE70D1BA6BDDD6C2DF58DC992
	Cvo8DLaQysuldQahY.dat	16.05.2008 16:20:36	585	77F1500E9D8A7255EC7BE9F1CA14556D
	Cvo8DLaQysuldQahY.hdr	16.05.2008 16:20:36	426	1FA03A394DE842700191BEE655F2B06D
	Cw3mxQqEqGfSV23mJ.dat	16.05.2008 16:20:34	956	6B70E5329220175251BA1A0B8D029645
	Cw3mxQqEqGfSV23mJ.hdr	16.05.2008 16:20:34	335	B068A2EBF3A5A9DCBD29F229EB5E9540

eventlog

Oxygen Forensic Suite 2010 Analyst

Device View Tools Service Help

Desktop | Search | Export | Print | Reset Filters | Help | Quick filter:

Event Log

Event info

Cook John
+79035841186
Outgoing

Type: SMS
Subject: Thanks! Have yo received my emai
Duration: 00:00:00
Time Stamp: 02.06.2010 13:43:07
MD5 Hash:
5d839378bd9fcc00c380c8e1028b0da5

Full Event Log | Answered calls | Missed calls | Dialed calls | SMS | Packet Data

Type	Number	Subject	Description	Call duration	Status	Remote party	Time Stamp
SMS	+79636041032		Short message	00:00:00	Delivered	Beards Michael	03.06.2010 12:05:35
SMS	Beeline	Звони бесплатно 0501! Поддержи ...	Short message	00:00:00	Delivered		03.06.2010 11:09:13
SMS	+79636041032	Thank you!	Short message	00:00:00	Delivered	Beards Michael	02.06.2010 14:48:02
Unknown	+79636041032	hello!	MMS	00:00:00	Pending	Beards Michael	02.06.2010 14:46:28
Packet	(no number)	Traffic in: 1,79 KB, out: 10,16 KB	Packet Data	00:00:11	Disconnected	BeeLine MMS	02.06.2010 14:46:20
SMS	+79636041032	I need your assistance	Short message	00:00:00	Delivered	Beards Michael	02.06.2010 14:26:38
SMS	+79636041032	Call me ASAP	Short message	00:00:00	Delivered	Beards Michael	02.06.2010 14:26:19
SMS	+79636041032	Hello!	Short message	00:00:00	Delivered	Beards Michael	02.06.2010 14:26:01
Packet	(no number)	Traffic in: 176,38 KB, out: 8,73 KB	Packet Data	00:02:52	Disconnected	BeeLine Internet	02.06.2010 13:45:24
SMS	+79647910398	Hello! Have you received my fax	Short message	00:00:00	Delivered	James Simon	02.06.2010 13:44:22
SMS	+79035841186	Thanks! Have yo received my emai	Short message	00:00:00	Sent	Cook John	02.06.2010 13:43:07
SMS	+79035841186	Ok. I'll call you back	Short message	00:00:00	Delivered	Cook John	02.06.2010 13:42:28
SMS	+79035841186	We need to discuss it a bit late	Short message	00:00:00	Sent	Cook John	02.06.2010 13:41:45
SMS	+79035841186	Hello! Please, call me tomorrow	Short message	00:00:00	Sent	Cook John	02.06.2010 13:41:06
Voice	+79035841186		Voice call	00:00:00		Cook John	02.06.2010 8:51:11
Voice	+79647910284		Voice call	00:00:04		Bobson Nick	01.06.2010 11:34:27
Voice	+79647910284		Voice call	00:00:03		Bobson Nick	01.06.2010 11:33:04
Voice	+79647910284		Voice call	00:00:00		Bobson Nick	01.06.2010 11:32:25
Voice	+79647910284		Voice call	00:00:04		Bobson Nick	01.06.2010 11:32:09
Voice	+79647910284		Voice call	00:00:06		Bobson Nick	01.06.2010 11:31:43
Voice	+79647910284		Voice call	00:00:00		Bobson Nick	01.06.2010 11:31:07
SMS	+79035841186	Ok	Short message	00:00:00	Sent	Cook John	01.06.2010 11:29:21
SMS	+79035841186	By email please	Short message	00:00:00	Delivered	Cook John	01.06.2010 11:28:59
SMS	+79035841186	Ok. I'll send it via fax	Short message	00:00:00	Sent	Cook John	01.06.2010 11:28:23
SMS	+79035841186	Annual report	Short message	00:00:00	Delivered	Cook John	01.06.2010 11:27:54
SMS	+79035841186	Do you nee any additional docume	Short message	00:00:00	Sent	Cook John	01.06.2010 11:27:19
SMS	+79035841186	Hello! Everything is allright. I've chec...	Short message	00:00:00	Delivered	Cook John	01.06.2010 11:26:29
SMS	+79035841186	Hello! How are you?	Short message	00:00:00	Sent	Cook John	01.06.2010 11:24:19
SMS	+79647910398	Bye!	Short message	00:00:00	Delivered	James Simon	01.06.2010 11:23:49
SMS	+79647910398	Ok. Bye	Short message	00:00:00	Sent	James Simon	01.06.2010 11:23:23
SMS	+79647910398	Oh don't worry. I'm a bit busy now	Short message	00:00:00	Delivered	James Simon	01.06.2010 11:23:09
SMS	+79647910398	Whats up?	Short message	00:00:00	Sent	James Simon	01.06.2010 11:22:13
SMS	+79647910398	No problem! Call me a bit later	Short message	00:00:00	Delivered	James Simon	01.06.2010 11:21:57
SMS	+79647910398	Good! Lets meet tomorrow	Short message	00:00:00	Sent	James Simon	01.06.2010 11:20:59
SMS	+79647910398	Fine thanks!	Short message	00:00:00	Delivered	James Simon	01.06.2010 11:20:23
SMS	+79647910398	Hi, Simon! How are you?	Short message	00:00:00	Sent	James Simon	01.06.2010 11:19:40
Voice	+79647910398		Voice call	00:00:17		James Simon	01.06.2010 11:16:52
Voice	+79647910398		Voice call	00:00:05		James Simon	01.06.2010 11:16:22
Voice	+79647910398		Voice call	00:00:08		James Simon	01.06.2010 11:15:57
Voice	+79647910398		Voice call	00:00:11		James Simon	01.06.2010 11:15:20
Voice	+79647910398		Voice call	00:00:00		James Simon	01.06.2010 11:14:23
Voice	+79647910398		Voice call	00:00:09		James Simon	01.06.2010 11:13:54

Desktop | New device (N73-1) | New device (N73-1) | New device (iPhone 3G)

Device Info
Phonebook
Calendar
Tasks
Messages
Event Log
File Browser
Extras

Analyst version: 2.8.0.534 | New device (N73-1) | Total: 106 | Filtered: 106 | MD5 Hash: 5d839378bd9fcc00c380c8e1028b0da5

messages

Messages

Oxygen Forensic Suite 2 - 1.5.0.2

Direction / Folder / MD5 Hash	Time stamp / Service Center Time Stamp	Remote party	Description / Message
Incoming Inbox F1CCF322F6F98DBFDECF1AA57E65762D	16.05.2008 13:08:49 N/A	+79262479174	Ok,i'll be there in 5 min.
Incoming Inbox 27333E2D5DB7A3A656759150FB5B04D6	16.05.2008 13:05:24 N/A	+79035841186	Formidable!
Incoming Inbox D966A88EB41E4D78897F8E9BFA67DF20	18.07.2007 11:32:30 N/A	+79052729910	Uj kak-to bolno merzko sie 6ou vygljadit.
Incoming Inbox 64E33AF06AC21591AEF858E6F0B56441	17.07.2007 23:49:42 N/A	+79052729910	To na zapade, a to u nas. Raznye javlenija. Ibo otblesk na nih istorija na6ej i ih civilizacii brosaet raznyj.
Incoming Inbox 0F4BDC2E6F61204723A0417D9FF86681	17.07.2007 23:40:20 N/A	+79052729910	A-aa! Da, nas4et gay-paradov ja stala podozrevat - slog znakomyj.
Incoming Inbox B67F2D5516C6947A05878F54D41B27F9	16.09.2005 14:46:48 N/A	+1340	Please, ask John to meet me in the airport. My plane arrives at 9 PM on Saturday. Otpravitel':81.195.194.203
Incoming Inbox F16308EA61C699577FE85BCACD8C664B	16.09.2005 14:45:35 N/A	+1340	There are only one day before we'll be together again. Hope, you didn't forget your sailor. I didn't.I miss you every minute. Otpravitel':81.195.194.203
Incoming Inbox E5FC1DA1BC9E3021F7C091005488D2E8	16.09.2005 14:44:49 N/A	+1340	The trip to the Pirate Bay was marvellous. I found a great gift for you in a store on a real pirat frigate. I'm sure, you'll like it! Otpravitel':81.195.194.203

Summary

- There’s a lot of information that can be retrieved from smart phones
- History
  - www, Chat/txt, Geolocation
    - People, pics, orientation
- Physical security is paramount
  - Forensic software can extract a lot IF you have physical access to the phone
- Ensure mobile device polices are enforceable

Addendum

- Some additional information on mobile phone security

10 Steps to Secure Mobile Devices

- Configure mobile devices
  - Enable auto-lock
  - Enable password protection
- Connect to secure Wi-Fi, disable when not in use
- Update OS frequently
- Use antivirus programs, configure auto updates
- Use encryption solution to keep portable data secure

10 Steps to Secure Mobile Devices

- Use digital certificates on mobile devices
- Take appropriate physical security measures
- Securely wipe your old phones
  - Delete everything
- Develop mobile device policies, procedures, standards, guidelines
- Increase user awareness

Acknowledgments

- Thanks to Lt. Col. Tim Buennemeyer for the use of some of his slides on PDA IDS and battery attacks.
- Thanks to John Paul Dunning for the section on Bluetooth security

references

- http://www.npr.org/2010/12/15/132058735/is-your-e-book-reading-up-on-you
- http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html

Contact Information

- Randy Marchany
- University IT Security Officer
- VA Tech IT Security Office & Lab
- 1300 Torgersen Hall
- Blacksburg, VA 24061
- 540-231-9523
- marchany@vt.edu
- http://security.vt.edu
- Twitter: @randymarchany

Virginia Information Technologies Agency

COV ITRM Mobile Device Policy

Bob Baskette

Senior Manager, Security Operations and Architect

COV ITRM Mobile Device Policy

- The draft policy is on ORCA for review and comment
- As of 7/2/2011 CSRM has received 97 comments from COV Agencies and Universities
- 20 of the comments request grammatical changes or formatting changes

COV ITRM Mobile Device Policy

- Major areas of interest based on comments
  - Use of removable media
  - Connecting to non-COV computing assets
  - Hardware and software restrictions
  - What constitutes a mobile device
  - What is COV data
  - Password policy
  - Use of personal devices

Use of Removable Media

- Installation and use of removable media for phones and tablets
  - Use of removable media is prohibited due to the lack of controls since the media cannot be wiped if not installed at the time of wiping instruction
  - Removable media is easily lost or stolen
- General Use of USB thumb drives
  - Covered in COV ITRM SEC 501-06
  - Not addressed in the Mobile Device Policy

Connecting to non-COV devices

- Connecting to Home/Public networks
  - Allowed if in compliance with the SEC 511 Telework Standard
- Connecting to Home/Public computers for charging
  - Not allowed since USB charging cables can transfer data as well as power
  - Car chargers are permitted

Hardware and Software restrictions

- What hardware components should be disabled by default:
  - GPS
  - Camera
  - Microphone
  - The list of enabled hardware should be approved by the Agency Head
- What software components should be disabled by default:
  - Web browsers
  - SMS/MMS programs

Mobile Device Definition

- A definition that properly describes a mobile device is difficult since the technology is ever evolving
  - Tablets and laptops are merging
  - Smart phones are replacing some laptops
- The draft Mobile Device Policy does not govern laptops or the removable media referenced in SEC 501
  - Mobile Device requirements will be added to a future version of SEC 501

COV Data

- COV data is any data that is provided to the Commonwealth for processing or storage by COV computing systems
  - COV email
  - COV form data
  - Working papers and documents
  - Data associated with web services
- Also includes configuration information
  - Must be included in the backup schedule

Password requirements

- The Mobile Device must adhere to the password requirements set forth in SEC 501 for length, complexity, lifetime, and history
  - Simple PINs are too easy to defeat prior to automated wiping windows
  - The device must use a password for screen lock and device configuration access

Use of Personal Devices

- The use of personal devices is a privileged granted by the Agency Head, not a right
  - The Acceptable Use Policy will stipulate the right of the Agency to remotely wipe a device without warning
  - The AUP will stipulate the right of the Agency to conduct a forensic review or the device
  - The AUP will also stipulate that the personal device cannot use customized firmware or allow the end user to escalate privilege

Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov

Thank You!

Virginia Information Technologies Agency

COV ITRM SEC 501-06: Important Changes

Bob Baskette

Senior Manager, Security Operations and Architect

COV ITRM SEC 501-06

- Publication Date
  - April 4, 2011
- Compliance Date
  - July 1, 2011 for revisions to the standard
- Supersedes
  - COV ITRM Standard SEC501-01 dated August 11, 2009 (revision: 5).

Document Legend

- Existing SEC 501-01v5 language
- Wording changes to clarify existing SEC 501-01v5 language
- New requirements

1.5. Exceptions to Security Requirements

- If an Agency Head determines that compliance with the provisions of this Standard or any related information security standards would adversely impact a business process of the agency, the Agency Head may request approval to deviate from a specific requirement by submitting an exception request to the CISO.

1.5. Exceptions to Security Requirements

- For each exception, the requesting agency shall fully document:
  - 1. The business need,
  - 2. The scope and extent,
  - 3. Mitigating safeguards,
  - 4. Residual risks,
  - 5. The specific duration, and
  - 6. Agency Head approval.

1.5. Exceptions to Security Requirements

- Each request shall be in writing to the CISO and approved by the Agency Head indicating acceptance of the defined residual risks. Included in each request shall be a statement detailing the reasons for the exception as well as mitigating controls and all residual risks. Requests for exception shall be evaluated and decided upon by the CISO, and the requesting party informed of the action taken.

1.5. Exceptions to Security Requirements

- An exception will not be accepted for processing unless all residual risks have been documented and the Agency Head has approved, indicating acceptance of these risks. The exception request must be submitted by the Agency Head or Agency ISO. Denied exception requests may be appealed to the CIO of the Commonwealth.

2.7. IT Security Audits

- 2.7.2.3. IT Security Audits should only be performed by independent parties who are not associated with the processes or procedures of the system.

4.3. IT System Hardening

- 4.3.2.9. Apply all software publisher security updates to the associated software products.

- 4.3.2.10. All security updates must be applied as soon as possible after appropriate testing, not to exceed 90 days for implementation.

4.3. IT System Hardening

- 4.3.2.11. Prohibit the use of software products that the software publisher has designated as End-of-Life (i.e., software publisher no longer provides security patches for the software product).

4.4. IT Systems Interoperability Security

Identify steps to protect data shared with other IT systems.

- 4.4.2.5. The written agreement shall specify that System Owners of the IT systems that share data acknowledge and agree to abide by any legal requirements (i.e., HIPAA) regarding handling, protection, and disclosure of the shared data, including but not limited to Data Breach requirements in this Standard.

4.7. Application Security

- 4.7.2.8. Agencies shall not use or store sensitive data in non-production environments (i.e., a development or test environment that does not have security controls equivalent to the production environment).

5.2 Account Management

- 5.2.2.6. Review all user accounts and corresponding privileges for the user's continued need to access all IT systems.

- 5.2.2.21. Require confirmation of the account request and approval by the IT system user's supervisor and approval by the Data Owner or designee to establish accounts for all sensitive IT systems.

5.3 Password Management

- 5.3.2.8. Require users of all sensitive IT systems, to include network systems, to change their passwords after a period of 90 days.

5.3.2.8 Password Management

- An Agency sponsoring an Internet-facing system containing sensitive data provided by private citizens, which is accessed by only those citizens providing the stored data, may determine the appropriate validity period of the password, commensurate with sensitive and risk.

5.3.2.8 Password Management

- The account holder must be provided with information on the importance of changing the account password on a regular and frequent basis.

5.3 Password Management

- 5.3.2.10. Configure all sensitive IT systems to maintain at least the last 24 passwords used in the password history files to prevent the reuse of the same or similar passwords.

5.3.2.10 Password Management

- An Agency sponsoring an Internet-facing system containing sensitive data provided by private citizens, which is accessed by only those citizens providing the stored data, may determine the appropriate number of passwords to be maintained in the password history file, commensurate with sensitive and risk.

5.3.2.10 Password Management

- The account holder must be provided with information on the importance of changing the account password on a regular and frequent basis.

5.3 Password Management

- 5.3.2.11. Provide a unique initial password for each new account of sensitive IT systems and require that the IT system user change the initial password upon the first login attempt.

5.32.11 Password Management

- An Agency sponsoring an Internet-facing system containing sensitive data provided by private citizens, which is accessed by only those citizens providing the stored data, may allow the citizen to continue to use the initial password so long as the Agency provides a mechanism to the citizen that allows the citizen to create a unique initial password.

5.3 Password Management

- 5.3.2.18. Implement a screen saver lockout period after a maximum of 30 minutes of inactivity for COV devices.

6.2 Data Storage Media Protection

- 6.2.2.3. Prohibit the storage of any Commonwealth data on IT systems that are not under the contractual control of the Commonwealth of Virginia. The owner of the IT System must adhere to the latest Commonwealth of Virginia information security policies and standards as well as the latest Commonwealth of Virginia auditing policies and standards.

6.2 Data Storage Media Protection

- 6.2.2.5. Prohibit the connection of any non-COV owned or leased data storage media or device to a COV-owned or leased resource, unless connecting to a guest network or guest resources. This prohibition, at the agency's discretion need not apply to an approved vendor providing operational IT support services under contract.

6.3 Encryption

- 6.3.2.3. Require encryption for the transmission of data that is sensitive relative to confidentiality or integrity over non-Commonwealth networks or any publicly accessible networks, or any transmission outside of the data's broadcast domain. Digital signatures may be utilized for data that is sensitive solely relative to integrity.

9.2 Threat Detection

- 9.2.2.6. Provide quarterly summary reports of IDS and IPS events to Commonwealth Security.

9.5 Data Breach Notification

- Medical information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

9.5 Data Breach Notification

1) Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

9.5 Data Breach Notification

2) An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov

Thank You!

Upcoming Events

Information Security System Association

ISSA

DATE: Wednesday, July 13, 2011

LOCATION: Maggiano's Little Italy
11800 West Broad Street, #2204, Richmond, VA 23233

TIME: 11:30 - 1:00pm. Presentation starts at 11:45.
Lunch served at 12.

COST: ISSA Members: $20 & Non-Members: $25

SPEAKER: TBD

TOPIC: *TBD*

Virginia Information Technologies Agency

MS-ISAC

National Webcast Initiative

Thursday, August 25

2:00 pm – 3:00 pm EDT

Topic: *Bring Your Own Device: Addressing the Security Challenges Of Employee-Owned Devices in the Workplace*

Visit MS-ISAC web for more information:

http://www.msisac.org/webcast/

Virginia Information Technologies Agency

Future ISOAG's

From 1:00 – 4:00 pm at CESC

Wednesday - August 3, 2011

Wednesday - September 7, 2011

ISOAG will be held the 1st Wednesday of each month in 2011

Future IS Orientation Sessions

Tuesday -	**September 13, 2011**	**9:00 – 11:30a (CESC)**
Tuesday -	**November 8, 2011**	**1:00 – 3:30p (CESC)**

IS Orientation is now available via webinar!

ISOAG-Partnership Update

IT Infrastructure Partnership Team
Bob Baskette

July 6, 2011

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

Crikey!!!

John Green is moving to Australia!!

Hide
Your
Vegemite!

ADJOURN

We Bid VITA's CISO,
John Green
a Fond Farewell &
Best Wishes