Forensics II

Cloud computing

Storebror 101

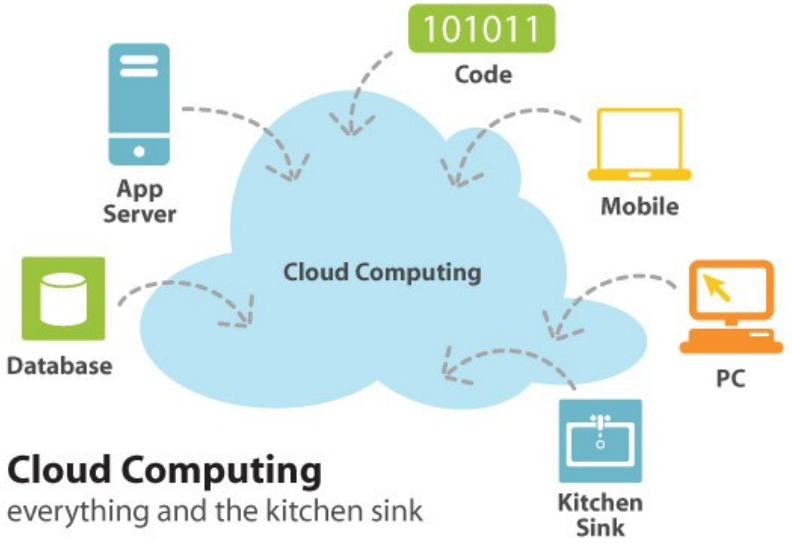
Digitala spårhundar – Data Mining

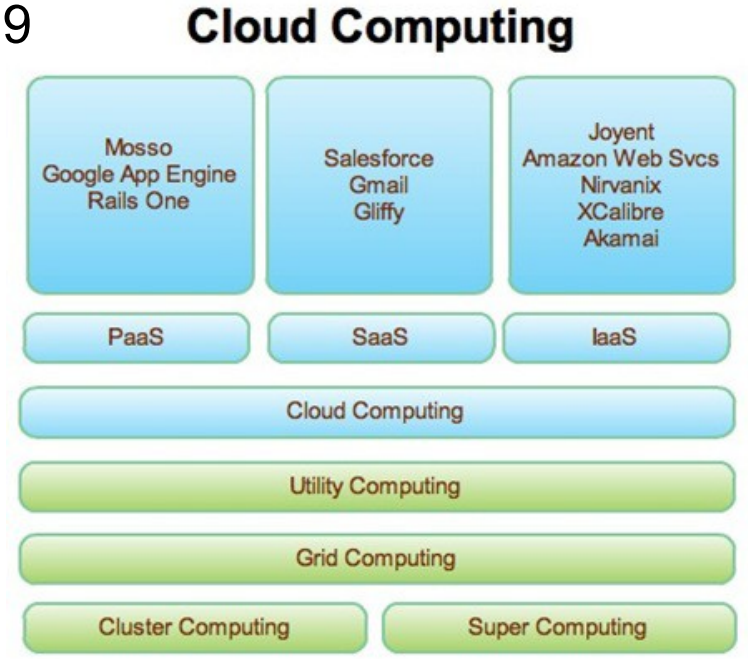
Expert vittne

Extra - Registry hashes etc.

Datormoln och Mobilitet

- X as a Service (XaaS) - term för hyr tjänster
  - **P**latform, **S**oftware and **I**nfrastructure
  - Ex. MicroSoft Office Web Apps and Google Apps
- Cloud computing - grid baserade system som gör XaaS möjligt
  - http://computersweden.idg.se/2.2683/1.202552/molnigt-varre
- 20% av företagen använde det i USA, 2009
- GIS is needed to localize suspect!?





1.0 In blue you have what is lately called Cloud Computing. In green, some of the underlying work done that led to Cloud Computing. At the top are examples of each XaaS type.

Amazon Web Services

AWS Management Conso | Google Calendar | Inkorgen (122) - jones.han

https://console.aws.amazon.com/console/home?#

Apps | Freja och Embla - O... | Synonymer.se - Lexi... | Folkets lexikon | Wiktionary, den fria ... | Google Translate | Android Developers ... | gotAPI/CSS - Instant... | Other bookmarks

Services | Edit | Global | Help

Amazon Web Services

Compute & Networking

- **Direct Connect** — Dedicated Network Connection to AWS
- **EC2** — Virtual Servers in the Cloud
- **Route 53** — Scalable Domain Name System
- **VPC** — Isolated Cloud Resources

Storage & Content Delivery

- **CloudFront** — Global Content Delivery Network
- **Glacier** — Archive Storage in the Cloud
- **S3** — Scalable Storage in the Cloud
- **Storage Gateway** — Integrates On-Premises IT Environments with Cloud Storage

Database

- **DynamoDB** — Predictable and Scalable NoSQL Data Store
- **ElastiCache** — In-Memory Cache
- **RDS** — Managed Relational Database Service
- **Redshift** — Managed Petabyte-Scale Data Warehouse Service

Deployment & Management

- **CloudFormation** — Templated AWS Resource Creation
- **CloudTrail** — User Activity and Change Tracking
- **CloudWatch** — Resource and Application Monitoring
- **Elastic Beanstalk** — AWS Application Container
- **IAM** — Secure AWS Access Control
- **OpsWorks** — DevOps Application Management Service

Analytics

- **Data Pipeline** — Orchestration for Data-Driven Workflows
- **Elastic MapReduce** — Managed Hadoop Framework
- **Kinesis** — Real-time Processing of Streaming Big Data

App Services

- **CloudSearch** — Managed Search Service
- **Elastic Transcoder** — Easy-to-use Scalable Media Transcoding
- **SES** — Email Sending Service
- **SNS** — Push Notification Service
- **SQS** — Message Queue Service
- **SWF** — Workflow Service for Coordinating Application Components

Additional Resources

Getting Started
See our documentation to get started and learn more about how to use our services.

Trusted Advisor
Best practice recommendations to save money, improve fault tolerance, increase performance, and close security gaps.

Service Health

All services operating normally.

Updated: Jan 14 2014 11:07:00 GMT+0100

Service Health Dashboard

Set Start Page

Console Home

AWS Marketplace
Find & buy software, launch with 1-Click and pay by the hour.

 Privacy Policy | Terms of Use | Feedback

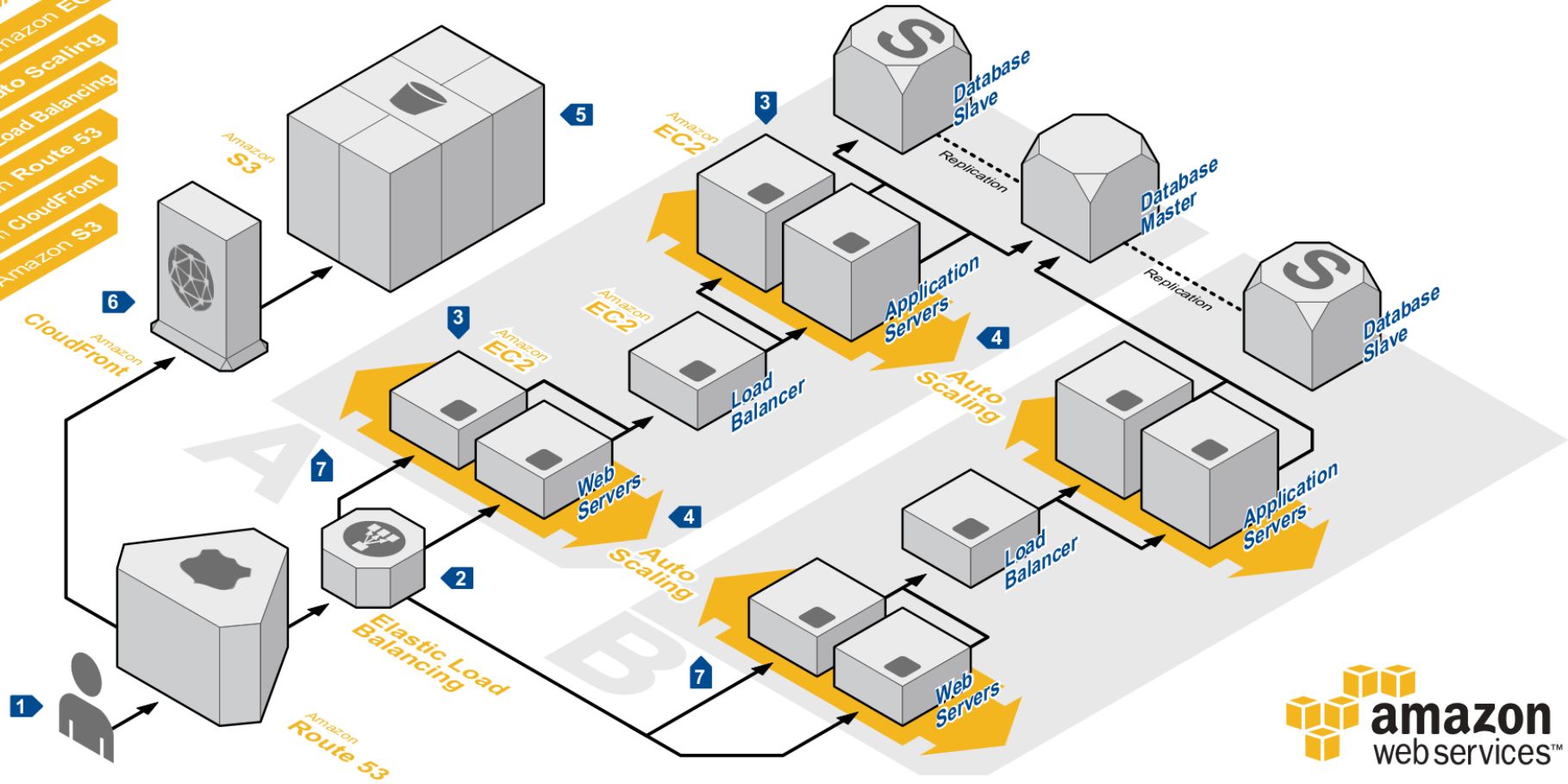
http://aws.amazon.com/architecture/

AWS Reference Architectures

Amazon EC2
Auto Scaling
Elastic Load Balancing
Amazon Route 53
Amazon CloudFront
Amazon S3

WEB APPLICATION HOSTING

Highly available and scalable web hosting can be complex and expensive. Dense peak periods and wild swings in traffic patterns result in low utilization rates of expensive hardware. Amazon Web Services provides the reliable, scalable, secure, and high-performance infrastructure required for web applications while enabling an elastic, scale out and scale down infrastructure to match IT costs in real time as customer traffic fluctuates.



amazon web services™

System Overview

1 The user's DNS requests are served by **Amazon Route 53**, a highly available Domain Name System (DNS) service. Network traffic is routed to infrastructure running in Amazon Web Services.

2 HTTP requests are first handled by Elastic Load Balancing, which automatically distributes incoming application traffic across multiple **Amazon Elastic Compute Cloud (EC2)** instances across Availability Zones (AZs). It enables even greater fault tolerance in your applications, seamlessly providing the amount of load balancing capacity needed in response to incoming application traffic.

3 Web servers and application servers are deployed on **Amazon EC2** instances. Most organizations will select an **Amazon Machine Image (AMI)** and then customize it to their needs. This custom AMI will then be used as the starting point for future web development.

4 Web servers and application servers are deployed in an **Auto Scaling** group. Auto Scaling automatically adjusts your capacity up or down according to conditions you define. With Auto Scaling, you can ensure that the number of **Amazon EC2** instances you're using increases seamlessly during demand spikes to maintain performance and decreases automatically during demand lulls to minimize costs.

5 Resources and static content used by the web application are stored on **Amazon Simple Storage Service (S3)**, a highly durable storage infrastructure designed for mission-critical and primary data storage.

6 Static and streaming content is delivered by **Amazon CloudFront**, a global network of edge locations. Requests are automatically routed to the nearest edge location, so content is delivered with the best possible performance.

7 **Availability zones (AZs)** are distinct geographic locations that are engineered to insulate against failures in other AZs. Multiple AZs are combined into a region. Here, the entire web application is deployed in two different AZs for high availability.

Amazon Elastic Compute Cloud (EC2)

- Use a prebaked instance Amazon Machine Image (AMI) or your own virtual machine instance
  - Many different AMI:s are available (OS and pre-installed applications)
- Service types
  - On-demand instance
  - Reserved instance
  - Spot instance
  - Dedicated instance

Micro Instance
613 MB memory
Up to 2 EC2 Compute Units (for short periodic bursts)
EBS storage only
32-bit or 64-bit platform
I/O Performance: Low
API name: t1.micro

- Instance types (theres a lot of types in between)
  - Micro, standard, high-memory, high-cpu, cluster compute and cluster GPU instances
- Cost of on-demand AWS-EC2 t1.micro with Windows 2008 server, SQL 2008 Express and IIS with ASP.NET 3.5 in EU West (Ireland) region is around $22/month

Amazon Simple Storage Service (S3)

- Amazon S3 is storage for the Internet. It is designed to make web-scale computing easier for developers.
- Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web.
- Write, read, and delete objects containing from 1 byte to 5 terabytes of data each. The number of objects you can store is unlimited.
- Each object is stored in a bucket and retrieved via a unique, developer-assigned key.
- Cost?
- Standard Storage Reduced Redundancy Storage
- First 1 TB / month $0.125 per GB $0.093 per GB
- ...

EC2 Management Consol | Google Calendar | Inkorgen (122) - jones.han

https://console.aws.amazon.com/ec2/v2/home?region=eu-west-1#Instances:

Apps | Freja och Embla - O... | Synonymer.se - Lexi... | Folkets lexikon | Wiktionary, den fria ... | Google Translate | Android Developers ... | gotAPI/CSS - Instant... | Other bookmarks

Services | Edit | Ireland | Help

- EC2 Dashboard
- Events
- Tags

INSTANCES
- Instances
- Spot Requests
- Reserved Instances

IMAGES
- AMIs
- Bundle Tasks

ELASTIC BLOCK STORE
- Volumes
- Snapshots

NETWORK & SECURITY
- Security Groups
- Elastic IPs
- Placement Groups
- Load Balancers
- Key Pairs
- Network Interfaces

AUTO SCALING
- Launch Configurations
- Auto Scaling Groups

Launch Instance | Connect | Actions

Filter: All instances | All instance types | Search Instances | 1 to 2 of 2 Instances

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
roadroid.com...	i-6c22af25	m1.medium	eu-west-1c	stopped		None	
windows2012	i-b61a54fd	m1.medium	eu-west-1a	running	2/2 check...	None	ec2-176-34-228

Instance: i-b61a54fd (windows2012) **Elastic IP: 176.34.228.203**

Description | Status Checks | Monitoring | Tags

Instance ID	i-b61a54fd	Public DNS	ec2-176-34-228-203.eu-west-1.compute.amazonaws.com
Instance state	running	Public IP	176.34.228.203
Instance type	m1.medium	Elastic IP	176.34.228.203
Private DNS	ip-10-64-177-158.eu-west-1.compute.internal	Availability zone	eu-west-1a
Private IPs	10.64.177.158	Security groups	quicklaunch-1. view rules
Secondary private IPs	-	Scheduled events	No scheduled events
VPC ID	-	AMI ID	Loading ami-db2a28af...
Subnet ID	-	Platform	windows
Network interfaces	-	IAM role	-
Source/dest. check	False	Key pair name	ec2etex
		Owner	738316572035
EBS-optimized	False	Launch time	2012-12-01T10:27:58.000Z (9815 hours)
Root device type	ebs	Termination protection	True
Root device	/dev/sda1	Lifecycle	normal
Block devices	/dev/sda1	Monitoring	basic
		Alarm status	None

Feedback

S3 Management Console | Google Calendar | Inkorgen (122) - jones.han

https://console.aws.amazon.com/s3/home?region=eu-west-1

Apps | Freja och Embla - O... | Synonymer.se - Lexi... | Folkets lexikon | Wiktionary, den fria ... | Google Translate | Android Developers ... | Other bookmarks

Services | Edit | Global | Help

Create Bucket | Actions | None | Properties | Transfers

All Buckets

Name
akiaipfi7xmhgdk3ibvq-etexbucket
akiaipfi7xmhgdk3ibvq-oldserver
akiaipfi7xmhgdk3ibvq-tmpstore

Bucket: akiaipfi7xmhgdk3ibvq-etexbucket

Bucket: akiaipfi7xmhgdk3ibvq-etexbucket
Region: Ireland
Creation Date: Wed Apr 17 21:27:13 GMT+200 2013
Owner: Me

- Permissions
- Static Website Hosting
- Logging
- Notifications
- Lifecycle
- Tags
- Requester Pays
- Versioning

 Privacy Policy | Terms of Use | Feedback

Compute Engine — Goog

https://cloud.google.com/products/compute-engine/

Apps | Freja och Embla - O... | Synonymer.se - Lexi... | Folkets lexikon | Wiktionary, den fria ... | Google Translate | Android Developers ... | Other bookmarks

Google Cloud Platform

Go to my console | Sign out

Search this site

Why Google | **Products** | Solutions | Customers | Developers | Support | Partners

Contact sales or **Try it now**

Compute Engine

Run large-scale workloads on virtual machines hosted on Google's infrastructure. Choose a VM that fits your needs and gain the performance of Google's worldwide fiber network.

Get Started

http://yourstory.com/2013/12/google-compute-engine-better-than-aws/

Features

High-performance virtual machines

Compute Engine's Linux VMs are consistently performant, scalable, highly secure and reliable. Supported distros include Debian and CentOS. You can choose from micro-VMs to large instances.

Powered by Google's global network

Create large compute clusters that benefit from strong and consistent cross-machine bandwidth. Connect to machines in other data centers and to other Google services using Google's private global fiber network.

(Really) Pay for what you use

Google bills in minute-level increments (with a 10-minute minimum charge), so you don't pay for unused computing time.

Load balancing

Native load-balancing technology helps you spread incoming network traffic across a pool of instances, so you can achieve maximum performance, throughput and availability at low cost.

Fast and easy provisioning

Quickly deploy large clusters of virtual machines with intuitive tools including a RESTful API, command-line interface and web-based Console. You can also use tools such as RightScale and Scalr to automatically manage your deployment.

Compliance and security

All data written to disk in Compute Engine is encrypted at rest using the AES-128-CBC algorithm. Compute Engine has completed ISO 27001, SSAE-16, SOC 1, SOC 2, and SOC 3 certifications, demonstrating our commitment to information security.

Google Compute Engine

Google Compute Engine: Virtual Machines at Google Scale

Scale, performance, and value. Run your workloads on Google's infrastructure, paying only for what you use.
Flexibility and an Open Environment. Launch virtual machines with a variety of configurations using layer 3 load balancing to distribute work loads, or manage your workloads with additional solutions that were developed with our ecosystem of partners like RightScale, OpsCode, and Puppet Labs.
Predictable Performance. Deploy your applications on an infrastructure designed for strong isolation of users' actions with access to consistently fast and dependable core technologies.
Strong Security. Use built-in data privacy and security capabilities with data encryption on disk.

Learn More

Try it now

1 Sign up

a. If you don't already have one, sign up for a Google account.
b. Create a Compute Engine enabled project via the Google Cloud Console.

2 Install the Cloud SDK

System requirements:

- Python 2.6.x or 2.7.x.
- Cygwin [Windows only].

gcutil is distributed as part of the Cloud SDK, which contains tools and libraries for managing resources on Google Cloud Platform.

Windows Azure: Microsoft

www.windowsazure.com/en-us/

Apps | Freja och Embla - O... | Synonymer.se - Lexi... | Folkets lexikon | Wiktionary, den fria ... | Google Translate | Android Developers ... | Other bookmarks

SALES: 020-889-875 | MY ACCOUNT | PORTAL | Search

Windows Azure

FREE TRIAL

SOLUTIONS PRICING DOCUMENTATION DOWNLOADS ADD-ONS COMMUNITY SUPPORT

Move faster

Save money

Integrate on-premises apps and data

Try for free

Learn what matters most for cloud security. Register for our complimentary webinar.

Never wait for servers or infrastructure again

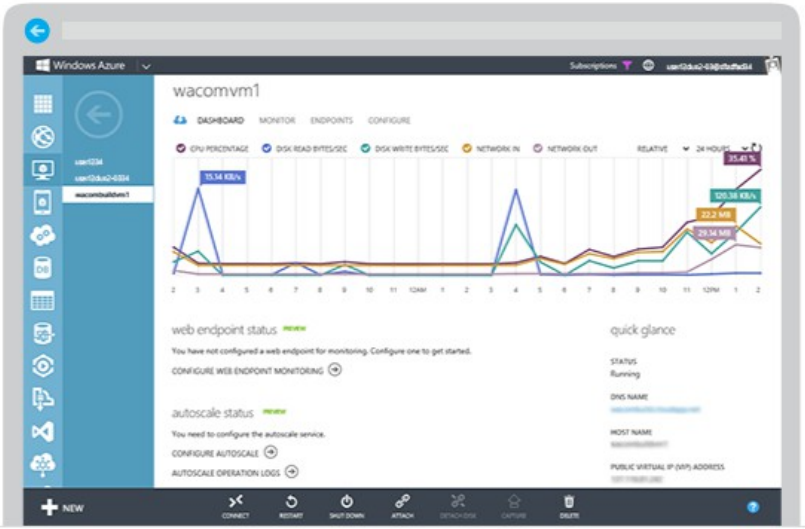
Instantly provision Windows and Linux VMs, apps, and infrastructure using Microsoft-managed datacenters in 13 regions around the world.

Learn more about Virtual Machines on Azure ▸

TREK

"With Azure, we don't have to worry about acquisition of new hardware or bigger networks. We can just make it happen."

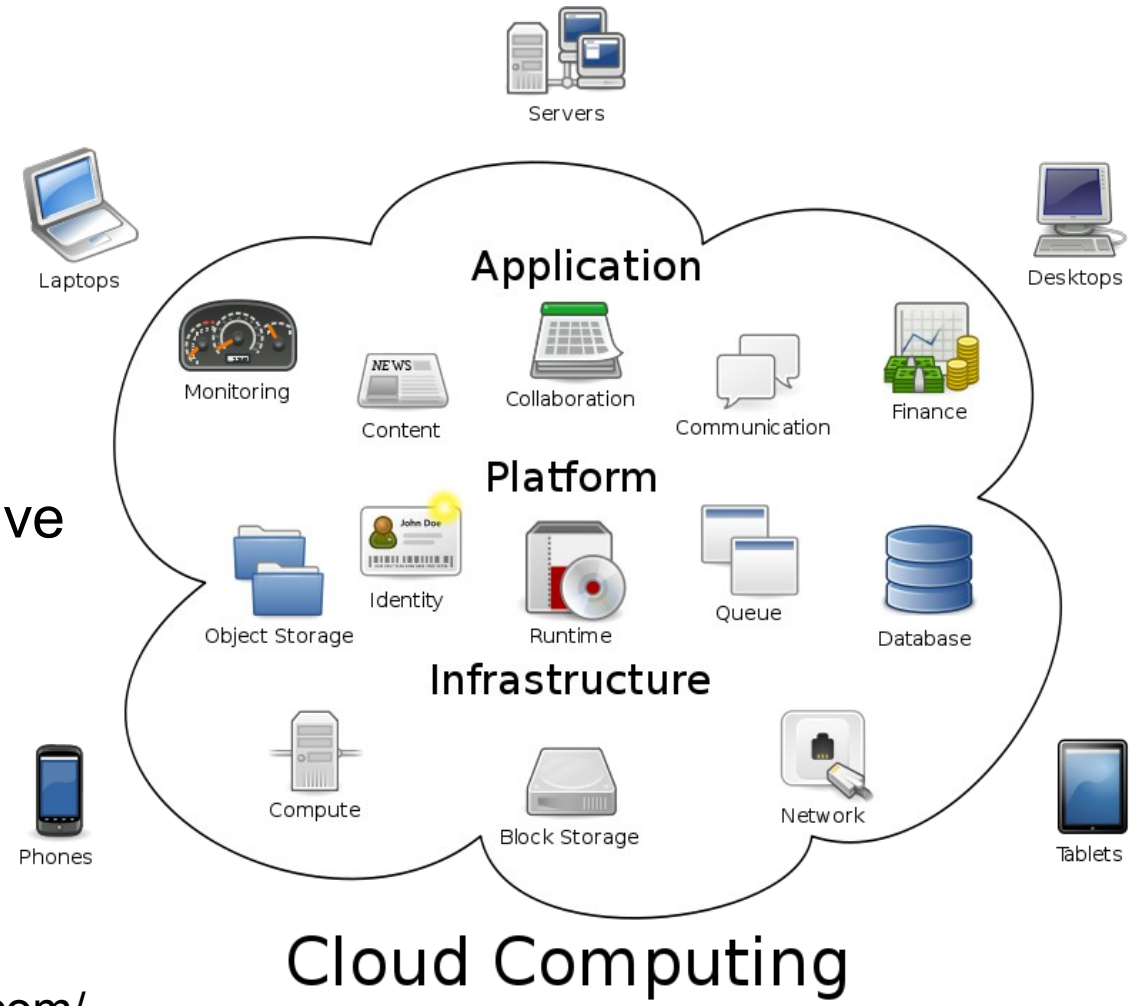
Steve Novoselac, IT Manager, Trek Bicycles



Other cloud services for private and corporate

- E-mail in general...
- Rackspace and IBM
- Amazon Cloud Drive
- Bitcasa
- Google Apps, Docs, Drive and App Engine
- MicroSoft Office 365 and Sky Drive
- Dropbox
- Idrive
- iCloud
- Box.net
- …

http://www.datacentermap.com/



Google Data Liberation Front

- Google Takeout
  - Export data from various supported services
  - https://www.google.com/settings/takeout

Service	Date "liberated"
Google Buzz	June 28, 2011[4]
Google Circles and Contacts	June 28, 2011[4]
Picasa Web Albums	June 28, 2011[4]
Google profile	June 28, 2011[4]
Google stream	June 28, 2011[4]
+1	July 15, 2011[6]
Google Tasks	August 1, 2011[7]
Google Voice	September 6, 2011[8]
Gmail Chat logs	September 15, 2011
Google Docs	January 24, 2012
Youtube	September 26, 2012
Google Calendar	December 5, 2013
Gmail	December 5, 2013[9]

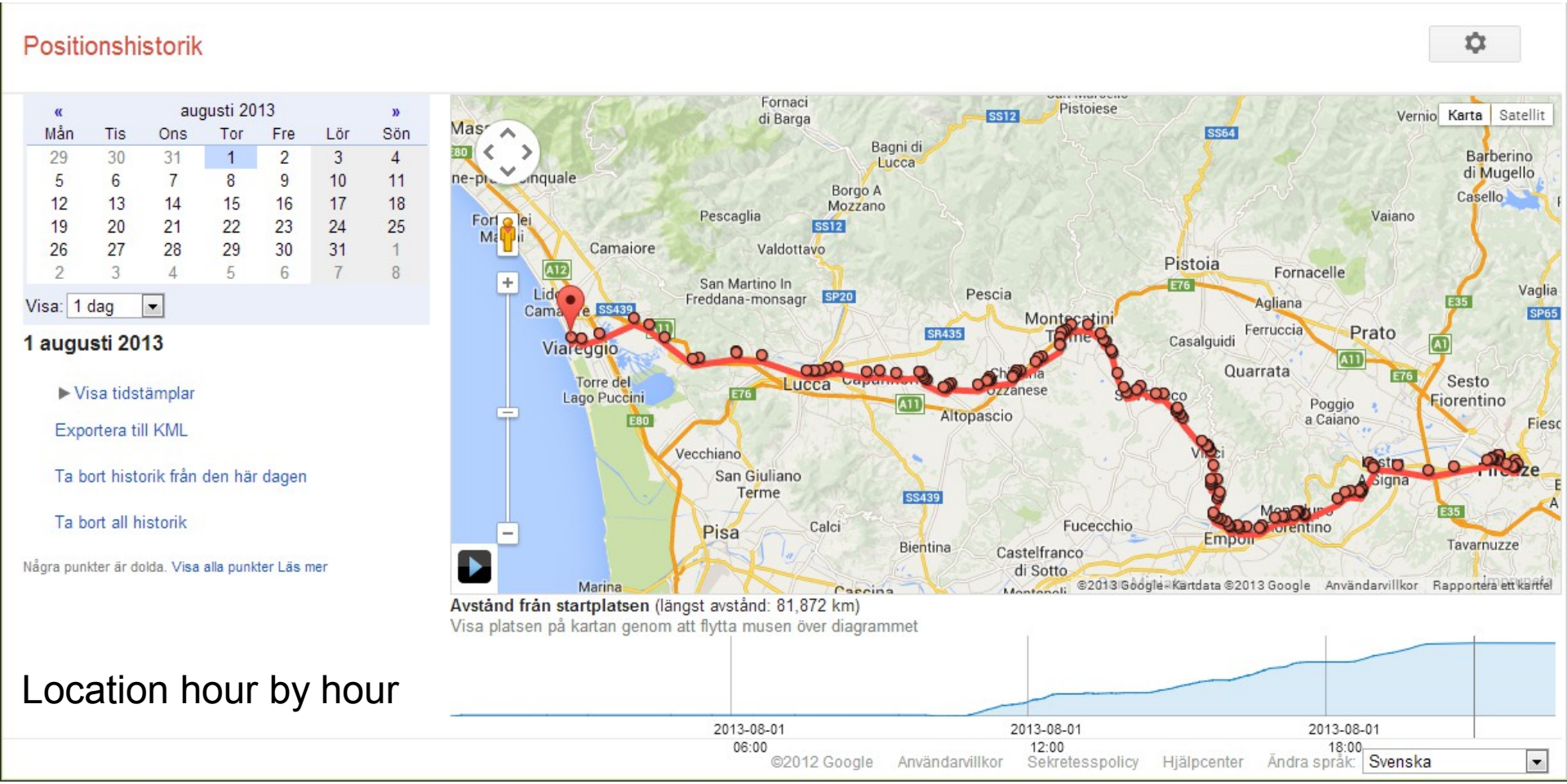
Create an archive

Supporting 17 products and counting...

- Bookmarks
- Contacts
- Profile
- Google+ Stream
- Messenger
- Panoramio
- Mail
- Drive
- Hangouts
- +1s
- YouTube
- Location History
- Calendar
- Voice
- Google+ Circles
- Google+ Pages
- Google Photos

Locationhistory via Gmail account

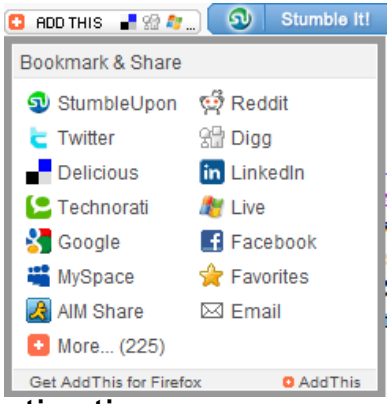
- If activated the phone collects location continiously
- https://maps.google.se/locationhistory



Location hour by hour

Social networking services

- Explosion of social networking sites in last years
  - Facebook, Google +, MySpace, Twitter, Bilddagboken, etc.
  - Many companies have joined (Yammer)
- Forensic profiling
  - Determining the strength of relationships
  - Analyzing the intent of actions given the pattern of use on a social networking site
  - Determining the likelihood of observable events being related
  - Uncovering past relationships
  - Archiving site privacy settings/policies
  - Forensic patterns of intra-social networking applications?
- Further reading
  - http://en.wikipedia.org/wiki/List_of_social_networking_websites
  - http://en.wikipedia.org/wiki/Use_of_social_network_websites_in_investigations
  - https://blogs.sans.org/computer-forensics/2009/06/11/facebook-forensics/

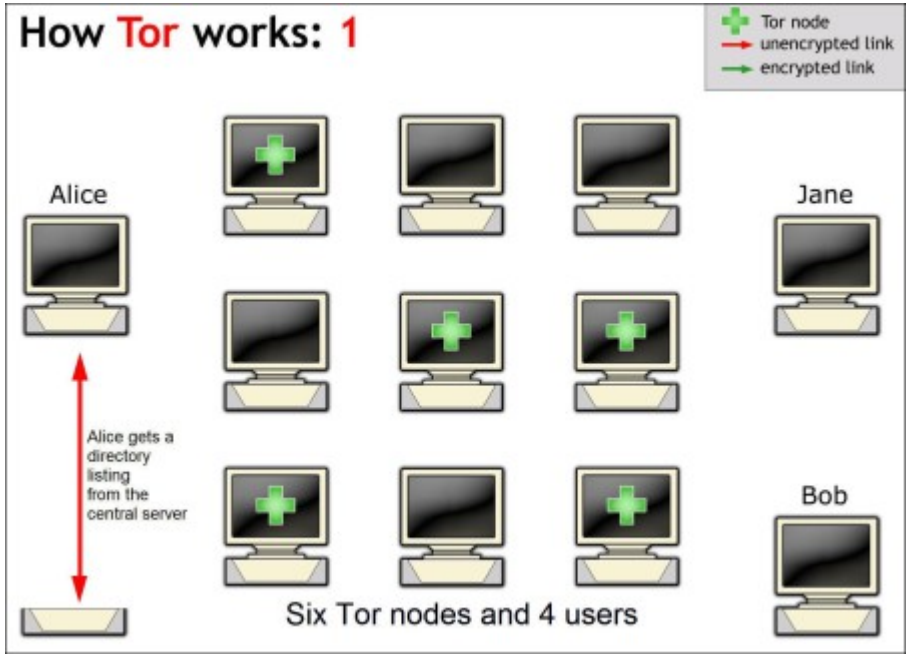


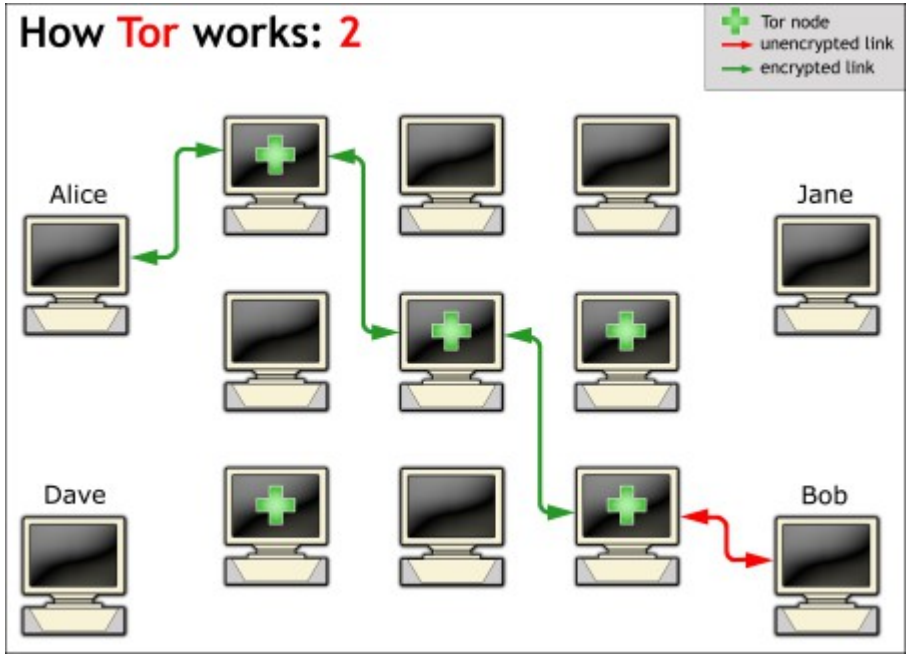
Virtualisering i olika former

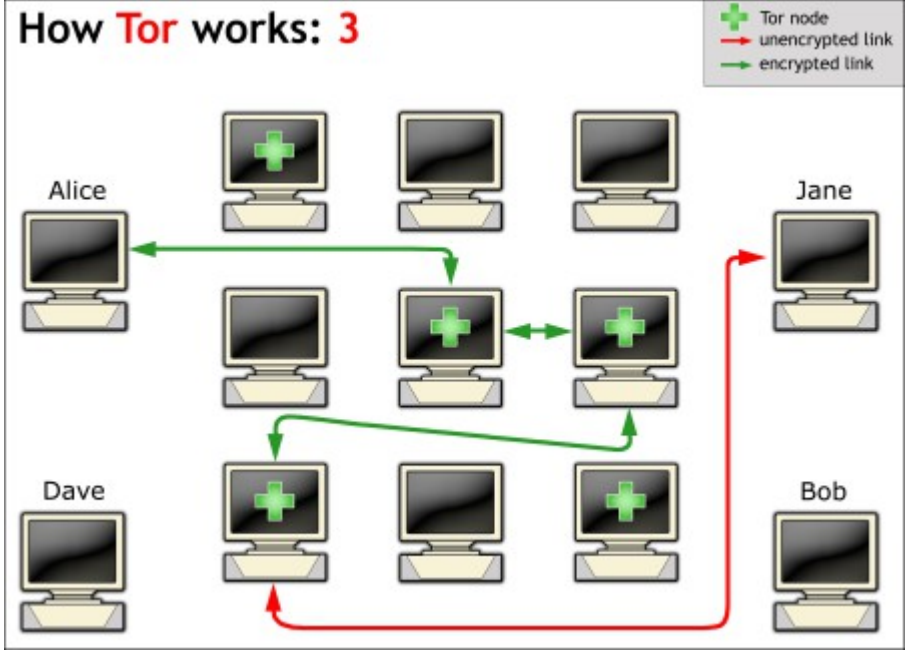
- Virtuella datorer/OS
  - På stark frammarch inom industrin sedan flera år
  - Forensiskt mest om att nyttja som verktyg i undersökningar
- Vad händer om en brottsling t.ex. kör VMware och trycker revert till snapshot efter varje session?
  - Kan man se något utanför VM?
    - Anslutna externa enheter (extern VM), trafik, registret, etc.
  - Finns något spår kvar i själva VM imagen (.VM*)?
    - Kryptering av config och suspend files etc?
      - http://communities.vmware.com/docs/DOC-10593;jsessionid=F53D9B06D009AAD6CFB443FB80ABDB4E
  - Tråd med länk till paper – ”Virtual Forensics” av Brett Shavers
    - http://www.forensicfocus.com/index.php?name=Forums&file=viewtopic&t=3379
- Virtuella världar
  - Spås öka mycket framöver (inte som filmen Surrogates :))
  - Second life, WOW, virtuella mötesplatser (kommersiella)

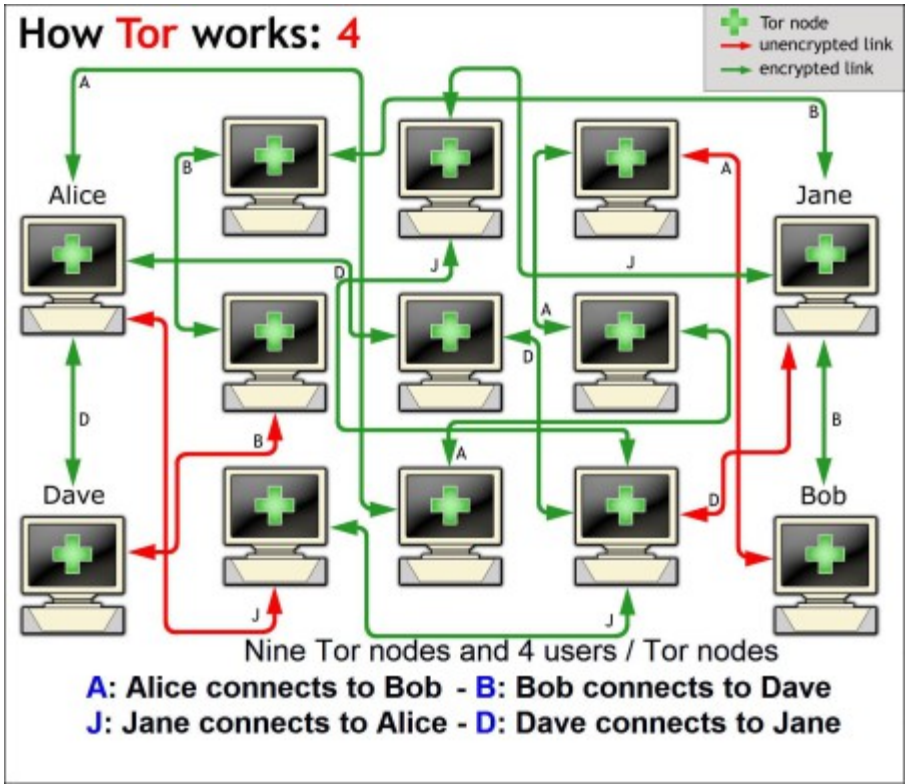
Onion routing

- Anonym på nätet?
- Målet med onion routing är att skydda integriteten för sändaren och mottagaren av ett meddelande, medans man samtidigt erbjuder ett skydd för meddelandet under tiden det skickas över nätverket
  - Each relay only know what relay sent its data and what relay it is going to send data to
  - Separate set of encryption keys for each hop
  - Route is changed every 10 minute
  - http://www.onion-router.net/
- TOR (The Onion Router)
  - http://www.torproject.org/
  - Last hop is unecrypted


How Tor works: 1
Tor node
unencrypted link
encrypted link
Alice
Jane
Alice gets a directory listing from the central server
Bob
Six Tor nodes and 4 users


How Tor works: 2
Tor node
unencrypted link
encrypted link
Alice
Jane
Dave
Bob


How Tor works: 3
Tor node
unencrypted link
encrypted link
Alice
Jane
Dave
Bob


How Tor works: 4
Tor node
unencrypted link
encrypted link
Alice
Jane
Dave
Bob
Nine Tor nodes and 4 users / Tor nodes
A: Alice connects to Bob - B: Bob connects to Dave
J: Jane connects to Alice - D: Dave connects to Jane

OneSwarm and followers

http://en.wikipedia.org/wiki/Oneswarm

- Anses vara efterföljaren till BitTorrent
  - Baserat på BitTorrent
- I ”princip säkert”
  - Distribuerad hash tabell (som magnet links)
    - http://en.wikipedia.org/wiki/Magnet_URI_scheme
  - RSA autenticering och kryptering av vänner, SSL kryptering av trafiken
- Ingen server, inga IP adresser, inga administratörer
- Man vet inte var filen man laddar ner kommer ifrån
  - http://www.nada.kth.se/~snilsson/public/OneSwarmFAQ.html
- Six degrees of separation
  - http://en.wikipedia.org/wiki/Six_degrees_of_separation

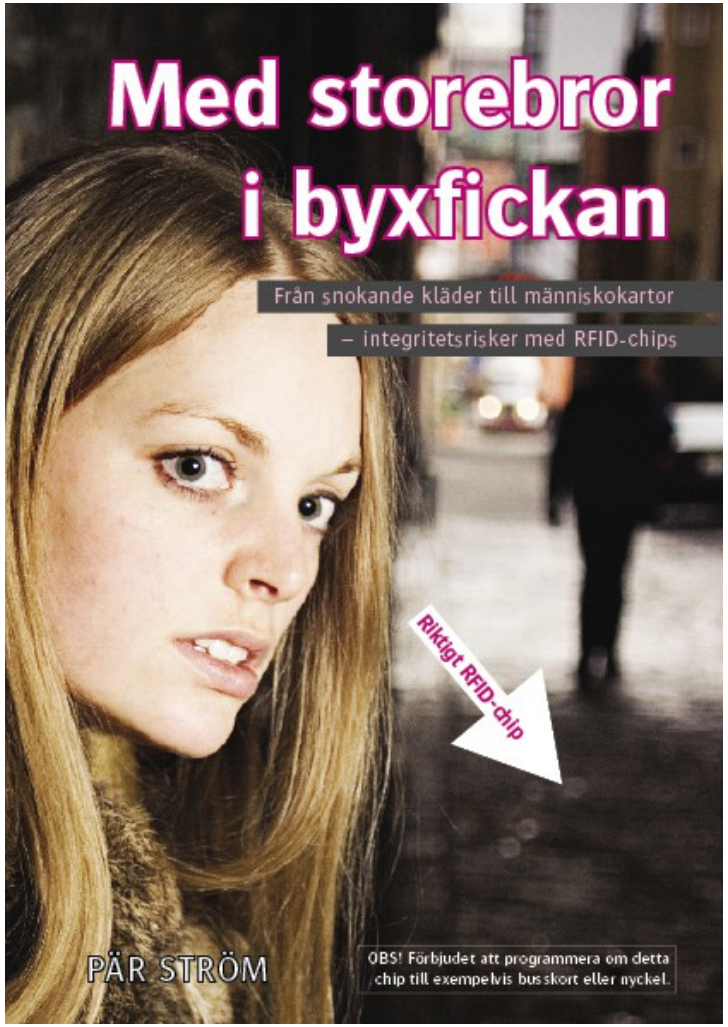
Storebror 101

- Nedlagd!
  - http://stoppastorebror.se/
- Den Nya Välfärden
  - http://www.dnv.se
  - Podcasts, pdf, mp3 m.m.
- NFC (Near Field Communication)
  - I 700 milj telefoner 2014
- RFID taggar
  - RFID med inbyggd sensor
    - http://www.sensiblesolutions.se/

I kissblöjan!
SensePad - den intelligenta blöjan


Storebror tar fram munkavlen
Internetfiltrering – censur som hotar yttrandefriheten
PÄR STRÖM


Integritetens
LILLA RÖDA
Så kan övervakning skada människor - Argumentsamling för storebrors kritiker
PÄR STRÖM


Med storebror i byxfickan
Från snokande kläder till människokartor – integritetsrisker med RFID-chips
Riktigt RFID-chip
PÄR STRÖM
OBS! Förbjudet att programmera om detta chip till exempelvis busskort eller nyckel.


MED STOREBROR I BAKSÄTET
Digital övervakning av dina bilfärder
PÄR STRÖM


22 TEKNOLOGIER SOM HOTAR DIN INTEGRITET
Med storebror i uppfinnarverkstan
Ny digital övervakning, från automatiska öron till internetdammsugare
PÄR STRÖM

Positioneringsspecial

- De vet var du är!
- Olika sätt att hålla koll
- Test av gps-trackers
- Framtidens tjänster för positionering
- Total kontroll med mobilen
- http://www.idg.se/2.1085/1.190260/positioneringsspecial

Digitala spårhundar gräver fram bevisen

- Nuix
  - Nuix grundades 1999 och har i dag cirka 50 anställda.
  - Nuix klarar av att hitta information som dolts inuti 1 000 rar-filer.
  - Nuix har en funktion som identifierar personer på bilder baserat på ansikts- och kroppsform. Den kan användas till att känna igen barnpornografiska bilder.
  - Tjänsten används i dag av olika myndigheter, advokatfirmor och polisstyrkor runt om i världen.
- SAS Institutes
  - SAS Institutes Text Analytics har väckt intresse hos myndigheter, som imponerades av hur Christopher Broxe kunde upptäcka kriminella aktiviteter helt utan förkunskap.
  - Text Analytics kräver att man etablerar en databas som kan användas som referens.
- Bägge tjänsterna undviker helt att begå dataintrång utan tar bara del av information som inte lösenordskyddats. Nuix kan identifiera lösenordsskyddat material, men ett tredjepartsprogram måste användas för att bryta sig in.

http://www.metro.se/metro-teknik/digitala-sparhundar-graver-fram-bevisen/Objjcq!12595/

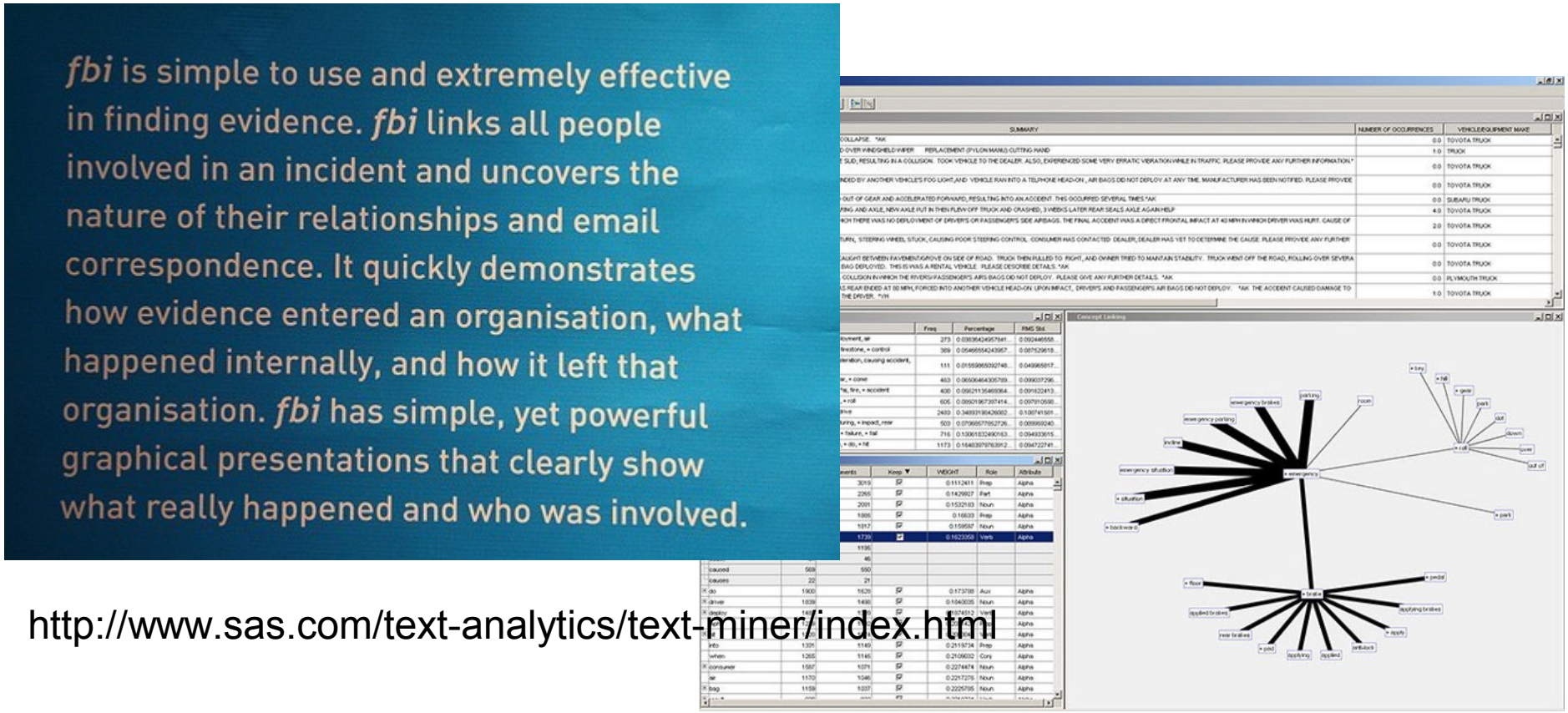
Datorstödd textanalys

- Textanalys är analys av ostrukturerad text. Textanalys arbetar bland annat med
  - Ordfrekvenser (vilka ord är vanligast i texten)
  - Viktning av ord (vissa vanliga ord är ointressanta, till exempel ”och”, ”att”)
  - Grammatiska regler (”springa” och ”sprang” ska räknas som samma ord)
  - Klungor av ord (vilka ord tenderar att stå nära varandra)
  - Taggning (vissa ord förses med märkord som kopplar dem till kategorier)
- Textanalys kan användas för att extrahera information ur stora textmassor eller för att hitta särskilt intressanta dokument eller inlägg
- http://www.idg.se/2.1085/1.312915/mer-an-tusen-ord

Nuix and Text Analytics

NUIX: FBI - advanced email and data forensics software
http://www.nuix.com/

Good forum topic
http://www.forensicfocus.com/index.php?name=Forums&file=viewtopic&t=1295

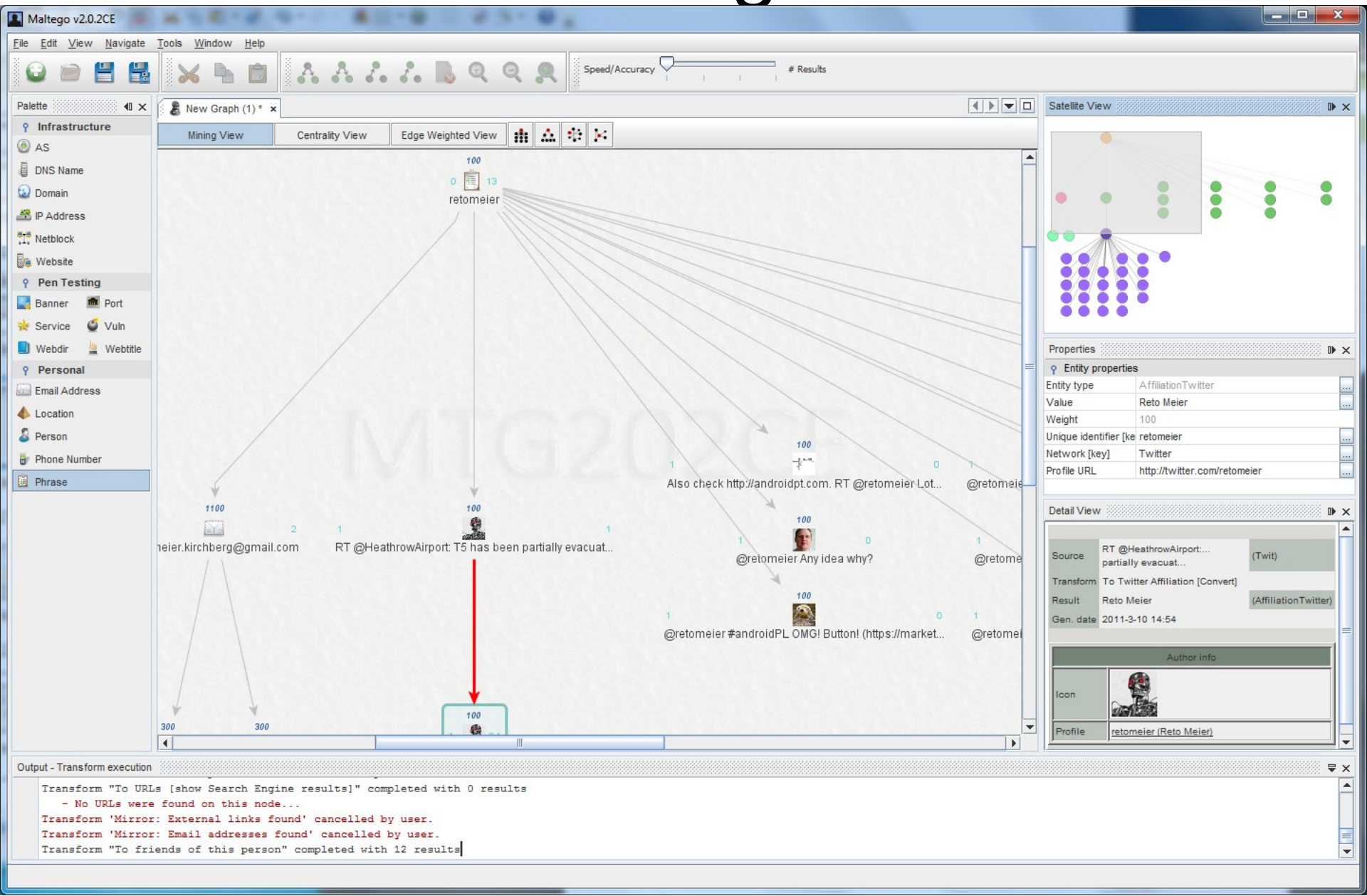


http://www.sas.com/text-analytics/text-miner/index.html

Nuix alternatives

- Aperture (free and doing 80% of Nuix work)
  - A Java framework for getting data and metadata
  - http://aperture.sourceforge.net/
  - Features
    - Crawl information systems such as file systems, websites, mail boxes and mail servers
    - Extract full-text and metadata from many common file formats
    - View files in their native applications
    - Ease of use: easy to learn, easy to code, easy to deploy in industrial projects
    - Flexible architecture: can be extended with custom file formats, data sources, etc., with support for deployment on OSGi platforms
    - Data exchange based on Semantic Web standards
- Manage Corporate Discovery > Discovery Attender
  - http://www.sherpasoftware.com/solutions/manage-discovery.shtml

Maltego

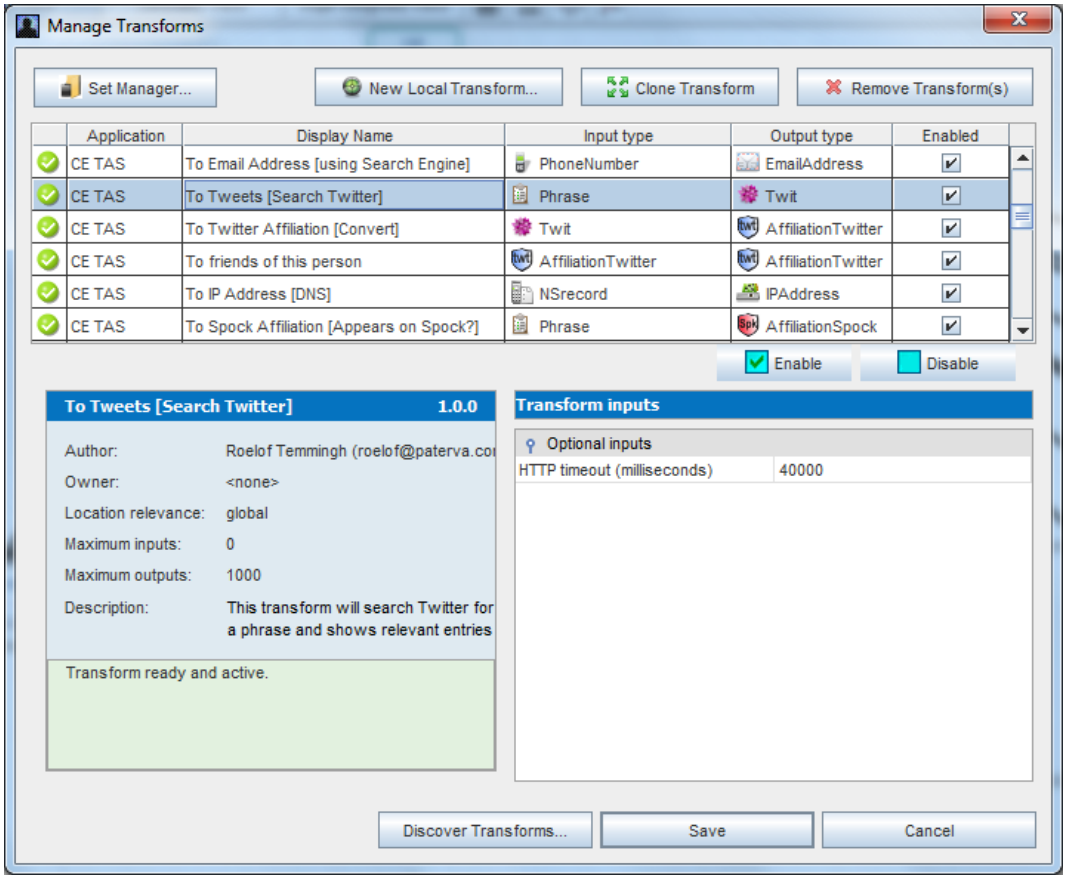

Maltego v2.0.2CE
File Edit View Navigate Tools Window Help
Speed/Accuracy
Results
Palette
Infrastructure
AS
DNS Name
Domain
IP Address
Netblock
Website
Pen Testing
Banner
Port
Service
Vuln
Webdir
Webtitle
Personal
Email Address
Location
Person
Phone Number
Phrase
New Graph (1) *
Mining View
Centrality View
Edge Weighted View
retomeier
Also check http://androidpt.com. RT @retomeier Lot...
@retomeier Any idea why?
@retomeier #androidPL OMG! Button! (https://market...
RT @HeathrowAirport: T5 has been partially evacuat...
Satellite View
Properties
Entity properties
Entity type AffiliationTwitter
Value Reto Meier
Weight 100
Unique identifier [ke retomeier
Network [key] Twitter
Profile URL http://twitter.com/retomeier
Detail View
Source RT @HeathrowAirport:... partially evacuat... (Twit)
Transform To Twitter Affiliation [Convert]
Result Reto Meier (AffiliationTwitter)
Gen. date 2011-3-10 14:54
Author info
Icon
Profile retomeier (Reto Meier)
Output - Transform execution
Transform "To URLs [show Search Engine results]" completed with 0 results
- No URLs were found on this node...
Transform 'Mirror: External links found' cancelled by user.
Transform 'Mirror: Email addresses found' cancelled by user.
Transform "To friends of this person" completed with 12 results

What is Maltego?

- Maltego is an information gathering tool that allows you to visually see relationships. Maltego allows you to enumerate network and domain information like
  - Domain Names, Whois Information, DNS Names
  - Netblocks, IP Addresses
- Maltego also allows you to enumerate People information like
  - Email addresses associated with a person's name
  - Web sites associated with a person's name
  - Phone numbers associated with a person's name
  - Social groups that are associated with a person's name
  - Companies and organizations associated with a person's name
- Maltego also allows you to
  - Do simple verification of email addresses
  - Search blogs for tags and phrases
  - Identify incoming links for websites
  - Extract metadata from files from target domains

Maltego

- All the information gathering "processes" that Maltego does are called "Transforms," and unfortunately not all of them are documented. But different transforms query different types of information. The full list is here:
  - http://ctas.paterva.com/view/Category:Transforms



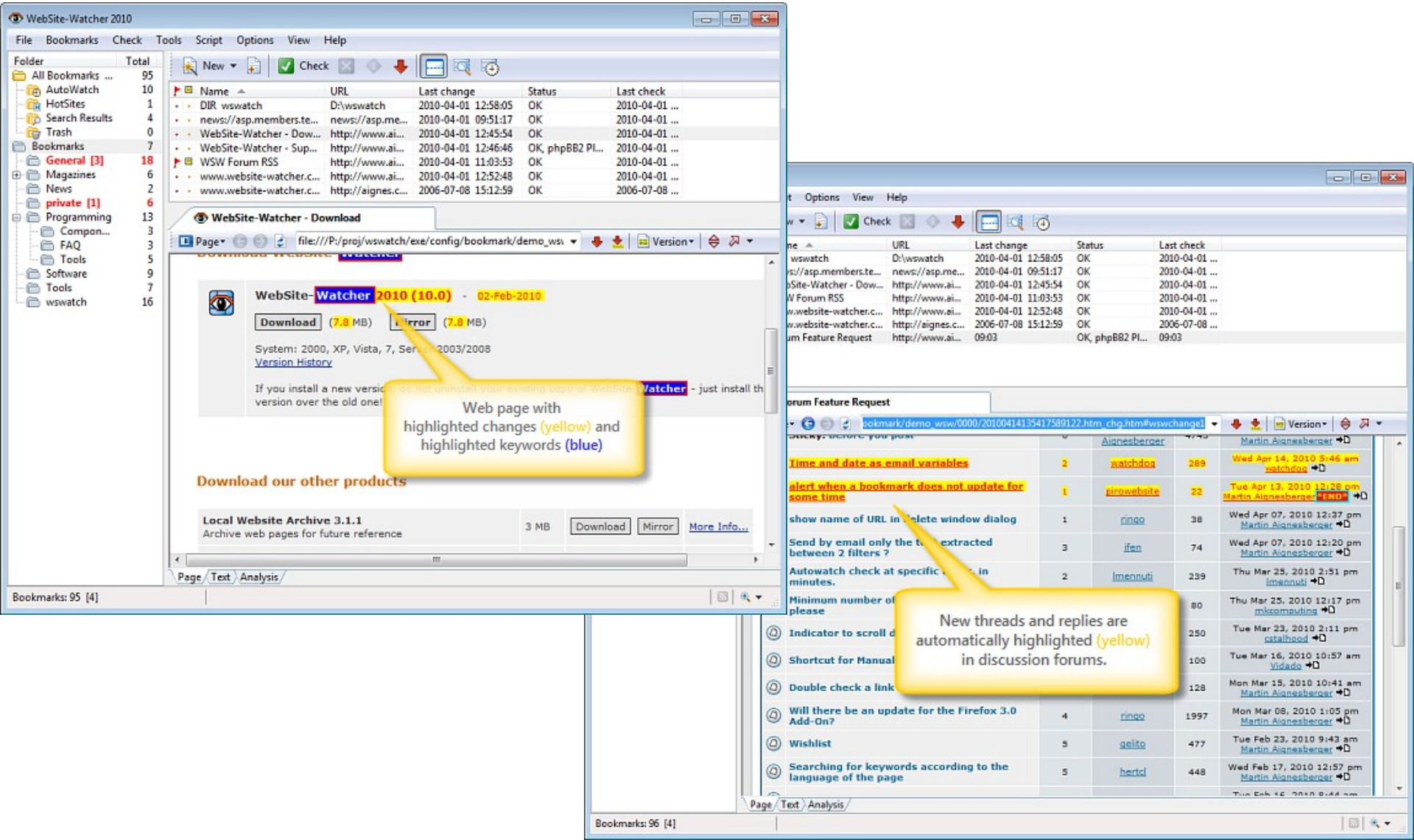
Maltego resources

- Maltego Part I - Intro and Personal Recon
  - http://www.ethicalhacker.net/content/view/202/24/
- Maltego Part II - Infrastructure Enumeration
  - http://www.ethicalhacker.net/content/view/251/24/
- Data Mining Tony Hawk's Twitter Hunt with Maltego
  - http://www.securityg33k.com/blog/?p=180
- Maltego: Transform & Correlate
  - https://www.issa.org/Library/Journals/2009/December/McRee-toolsmith.pdf
- Maltego
  - http://www.paterva.com

WebSite-Watcher 1

- Automatically check web pages for updates and changes
- Automate your daily routine, boost your productivity
- Features
  - Monitor web pages
  - Monitor password protected pages
  - Monitor forums for new postings and replies
  - Monitor RSS feeds, Newsgroups and local files
  - Highlight changes in a page
  - Powerful filter system to ignore unwanted content
  - Many more features to stay up-to-date!
  - http://aignes.net/

WebSite-Watcher 2



Expertvittne

- Läses på egen hand, se readings
  - Expert Witness and Report Writing.ppt
  - Computer Forensics Report.doc
  - http://users.du.se/~hjo/cs/dt2005/readings/
- Innehåll
  - Selecting and preparing an Expert Witness
  - 10 Mistakes an Expert Witness makes
  - Example expert witness
  - Example expert witness report

Windows Biometric Framework (WBF)

- The Windows Biometric Framework (WBF) provides an API which allows applications to use fingerprint devices to enroll, identify and verify user identities without gaining direct access to any biometric fingerprint hardware or samples
- The WBF can be used with fingerprint devices that have Windows Biometric Device Interface (WBDI) drivers
- The WBF is pluggable and extensible through plug-in adapters that manages sensor communications, biometric matching and templates storage. This ensures that the WBF can be used with a wide range of fingerprint sensors
- In Windows 7, the WBF will allow fingerprint readers to be used for authentication during UAC and Window logon
- Read more:
  - http://www.windowsvistaplace.com/vista/authentec
- Demo:
  - http://www.codeplex.com/BioApprovalWorkflow

Offline extraction of credentials from Windows registry hives 1

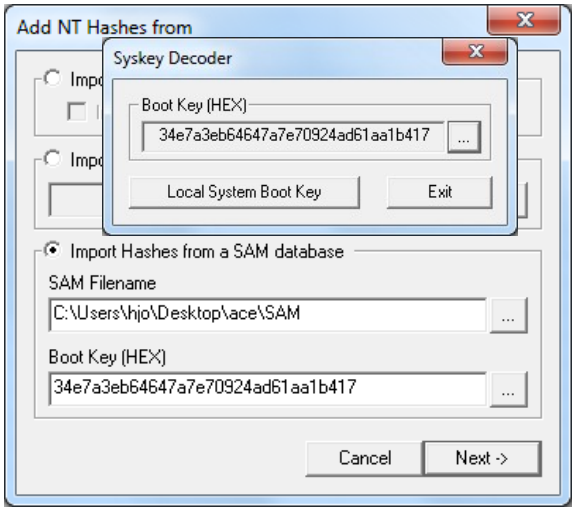
- Extract MD4/DES NT/LM-hash from: SAM\SAM\Domains\Account\Users\[RID]
- Both are obfuscated/encrypted in the V[] value, by using a SysKey (boot key)
- The boot key is found in 4 separate keys in the hive: SYSTEM\CurrentControlSet\Control\Lsa\{JD,Skew1,GBG,Data}
- The actual data needed is stored in a hidden field of the key that cannot be seen using tools like regedit, the 16-byte boot key also needs unscrambling
  - The boot key is also used for several other things as decrypt Local Security Authority(LSA) secrets and cached domain credentials etc.
- We then generate a RC4 key using a F[offset(x-y)] value from the hive: SAM\SAM\Domains\Account + bootkey and 2 constant strings which are MD5:ed
- The RC4 key is then used to decrypt 32 bytes from F[offset(k-n)] which finally generates the hashed boot key which we will use to derive the encryption keys for the individual users hashes
- In order to decrypt the users hash we again generate a RC4 key (algorithm is almost as before) and at last we can decrypt the users LM and NT hashes with RC4 using their respective users keys (phew!)
- The last stage needed is the pre-W2K algorithm – Sid2Key and DES decrypt

Offline extraction of credentials from Windows registry hives 2

syskey.exe

- Method fully described in article ”Syskey and SAM” at: http://moyix.blogspot.com/2008/02/syskey-and-sam.html
- Creddump (Python scripts)
  - LM and NT hashes (Syskey protected 128 bits)
  - Cached domain credentials and LSA secrets
  - http://code.google.com/p/creddump/
- Other tools
  - Cain [demo] – from Forensic 1 lab 4.8
    - Add NT Hashes, Syskey Decoder (System), ...
  - SAMInside
  - Bkhive, Samdump2 etc.
- Tutorials: IronGeek

http://www.irongeek.com/i.php?page=security/cracking-windows-vista-xp-2000-nt-passwords-via-sam-and-syskey-with-cain-ophcrack-saminside-bkhive-etc



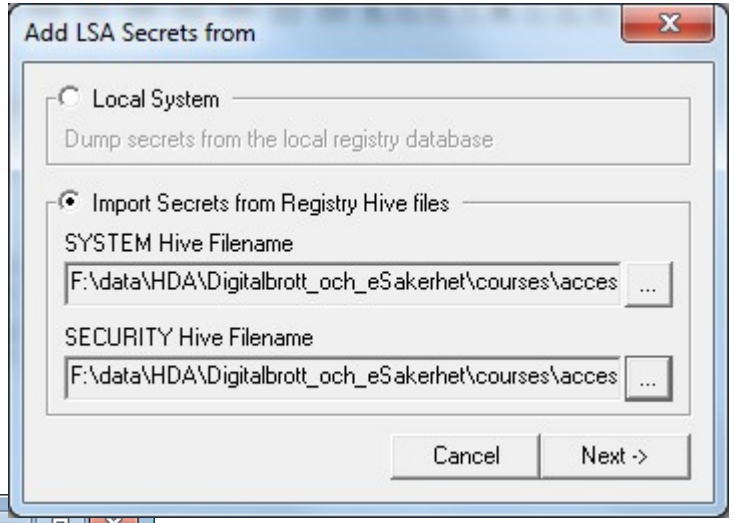
http://www.insidepro.com/

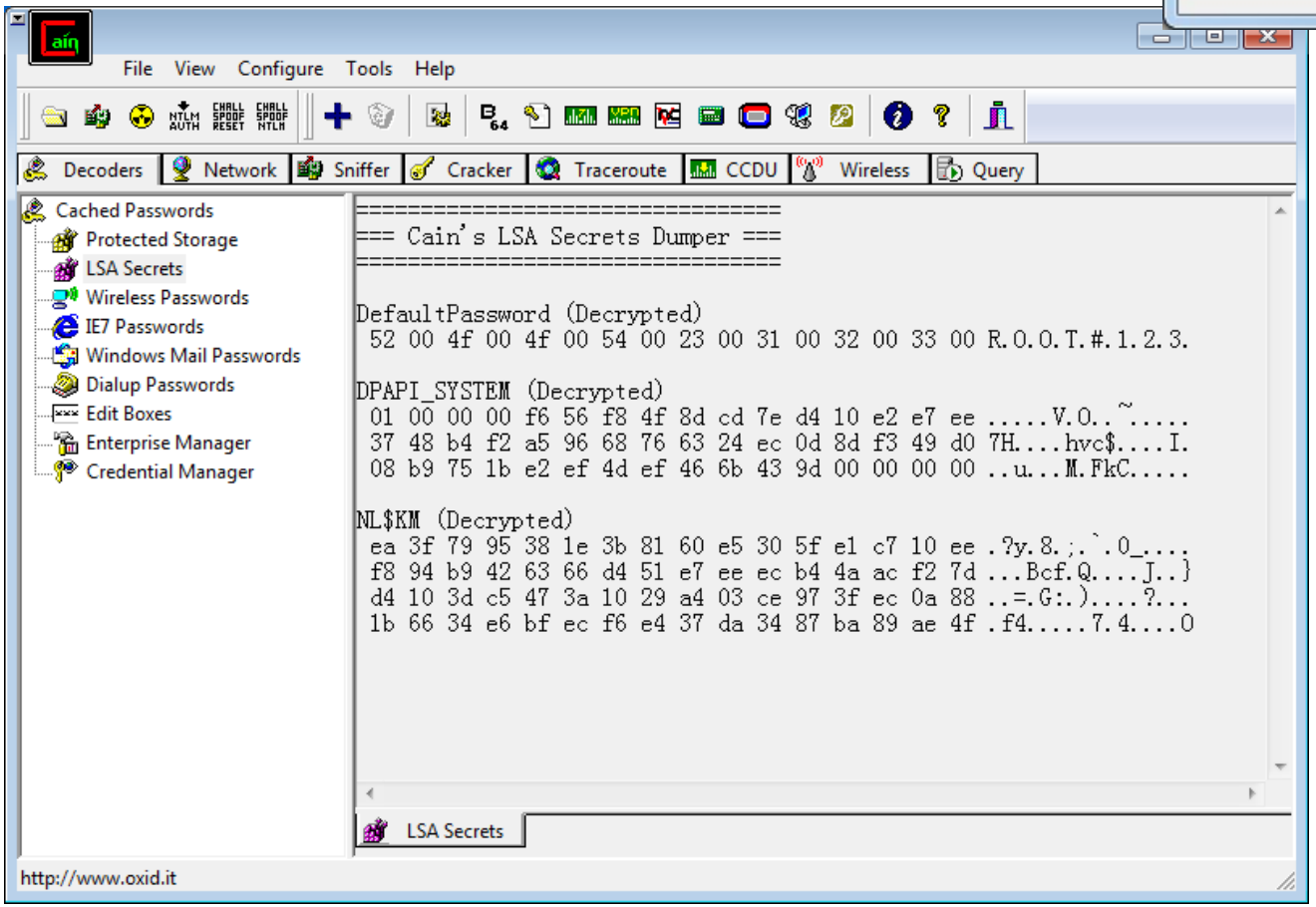
Offline extraction of credentials from Windows registry hives 3

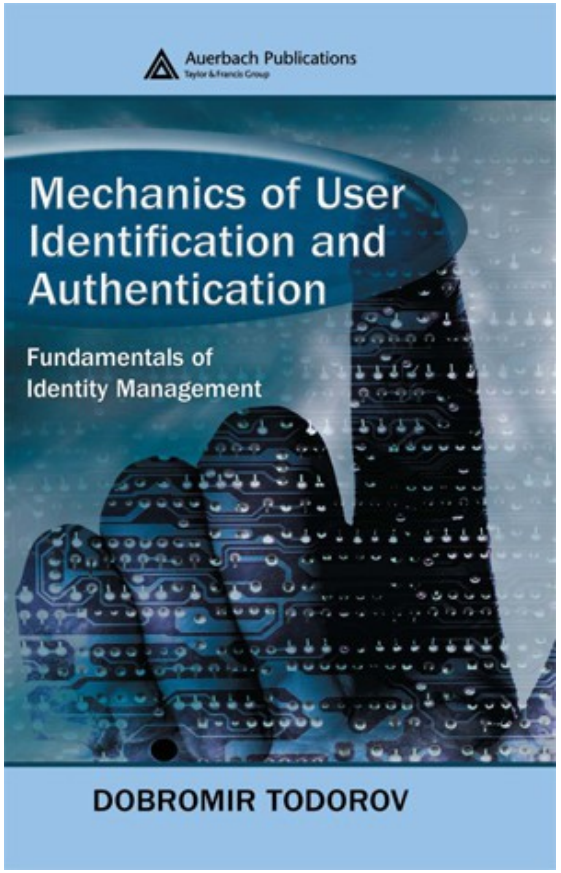
- Decrypting Local Security Authority (LSA) secrets you may find
  - DefaultPassword – used if auto-login is enabled
  - NL$KM – secret key used to encrypt cached domain passwords
  - Various service account secrets, $MACHINE.ACC, etc...
- LSA secrets are stored in SECURITY\Policy\Secrets and each encrypted secret have its own subkey
  - With subkeys as: CurrVal, CupdTime, OldVal, OupdTime, and SecDesc
  - [12 bytes of metadata] + [variable length of encrypted data]
- Decrypting the LSA secrets use the undocumented SystemFunction005 in advapi32.dll which is using DES in ECB mode to decrypt
- Algorithm below to obtain and calculate the LSA key which is derived from SECURITY\Policy\PolSecretEncryptionKey and the boot key
  - Obtain an RC4 key from the MD5 hash of the boot key followed by 1000 instances of bytes 60 to 76 of the data in PolSecretEncryptionKey
  - Use the RC4 key to decrypt 48 bytes of data from PolSecretEncryptionKey starting at offset 12
  - Bytes 0x10 through 0x20 of the resulting string is the value of the LSA key!

Cain LSA secrets

- DPAPI_SYSTEM is a legacy backup key that is used to recover DPAPI data
- Very good book describing algorithms

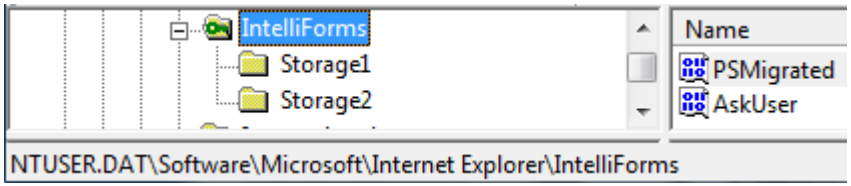






Break MS DPAPI (Data Protection Application Programming Interface)

- DPAPI is built in Windows since Win2K
  - http://en.wikipedia.org/wiki/Data_Protection_API
- DPAPI (Vista/IE7 and up) is the successor of the legacy PSSP (Protected Storage System Provider) which store (below) and moved to IntelliForms key
  - Form data, Web search queries, Web passwords and Outlook/Express passwords (PSSP are on the fly decrypted by RV)
  - Storage1 - queries and form data
  - Storage2 - login password info



- To break DPAPI protected data we need: user logon password, users protect folder and information specific below
  - For URL logon pages: the address of the page accessed
  - For search terms: the query engine header
  - For form data: the field name of the form field used
  - The AccessData PDF “Decrypting IntelliForms” have instructions performing the DPAPI information decryption with PRTK at their support web
- DPAPI programming example with a C++ wrapper class
  - http://www.codeproject.com/KB/system/protected_data.aspx

Class Identifier (CLSID)

- CLSID identifies applications and processes to Windows through registration in the software registry and the Classes subkey which is mapped to the HKEY_CLASSES_ROOT hive
  - A central point in how Windows uses to identify files and which application that access them
- Each application registers itself to the CLSID hive with a GUID and when OS needs to open a file etc. it can look it up and obtain the information needed to handle it
- Almost everything have a GUID in Windows - even Recycle Bin
  - COM and OLE technologies are dependent of this
  - Developers needs to define their own GUIDs/CLSIDs or search for valid GUIDs/CLSIDs when they use 3rd party objects as ActiveX controls etc.

  http://www.spywareguide.com/articles/open_letter_to_software_develo_53.html
- Registry viewer can generate a HTML report of file types and associated files
  - Report > Generate File Type Report

MS UVCview

- The viewed USB device data is not included in an image
- If serial number do not exist the PnP manager create a serial in registry having a “&” as second digit