Beyond files forensic
OWADE cloud based forensic

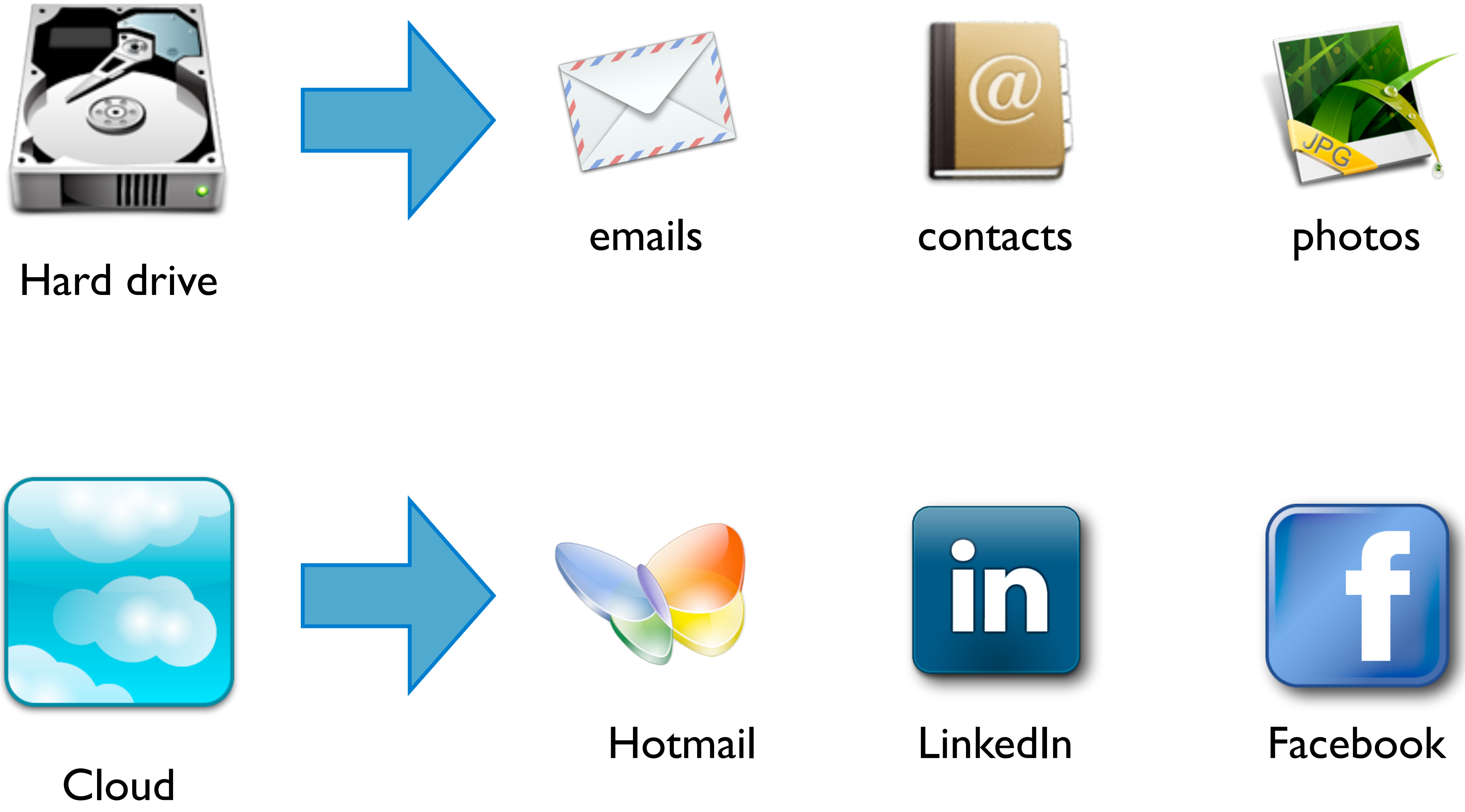
Elie Bursztein *Stanford University*
Ivan Fontarensky *Cassidian*
Matthieu Martin *Stanford University*
Jean Michel Picod *Cassidian*

The world is moving to the cloud

2.7 millions photos are uploaded to Facebook every 20 minutes

100 millions new files are saved on Dropbox every day

Data are moving to multiple services



Hard drive

emails

contacts

photos

Cloud

Hotmail

LinkedIn

Facebook

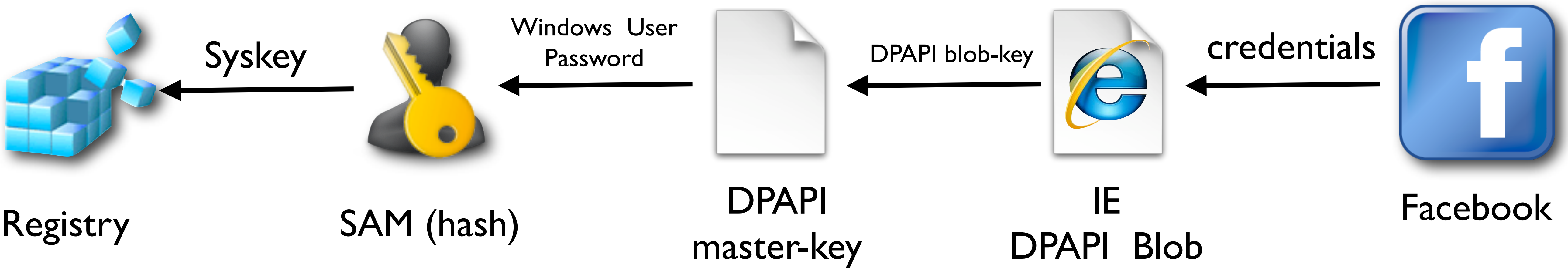
Impact on the forensic field

- There are more data which are harder to reach
- Dealing with cloud data force us to reinvent forensic

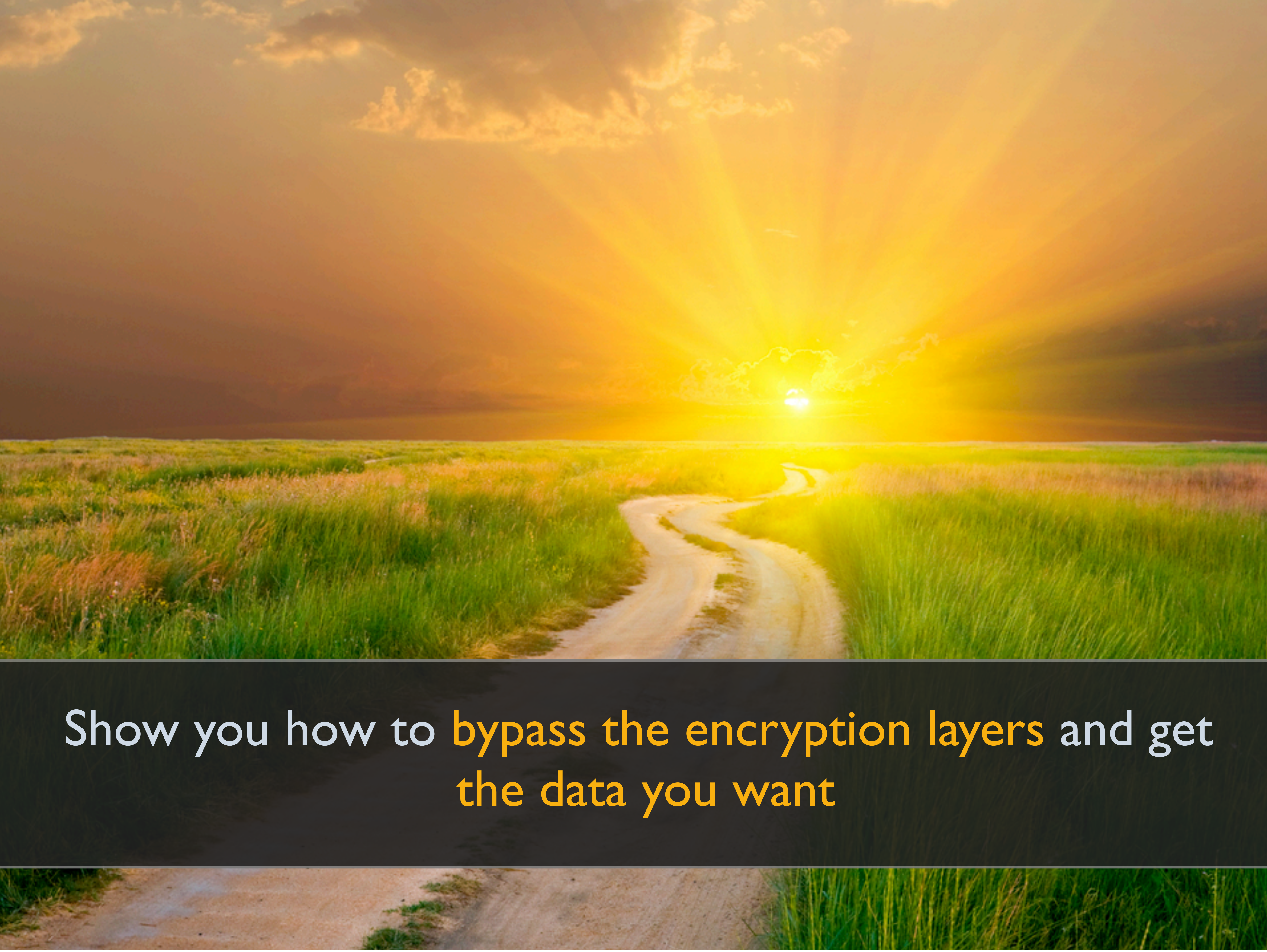
Let’s do cloud forensics

What is cloud forensics ?

Facebook credentials as a use case



Getting Facebook credentials require to bypass 4 layer of encryption



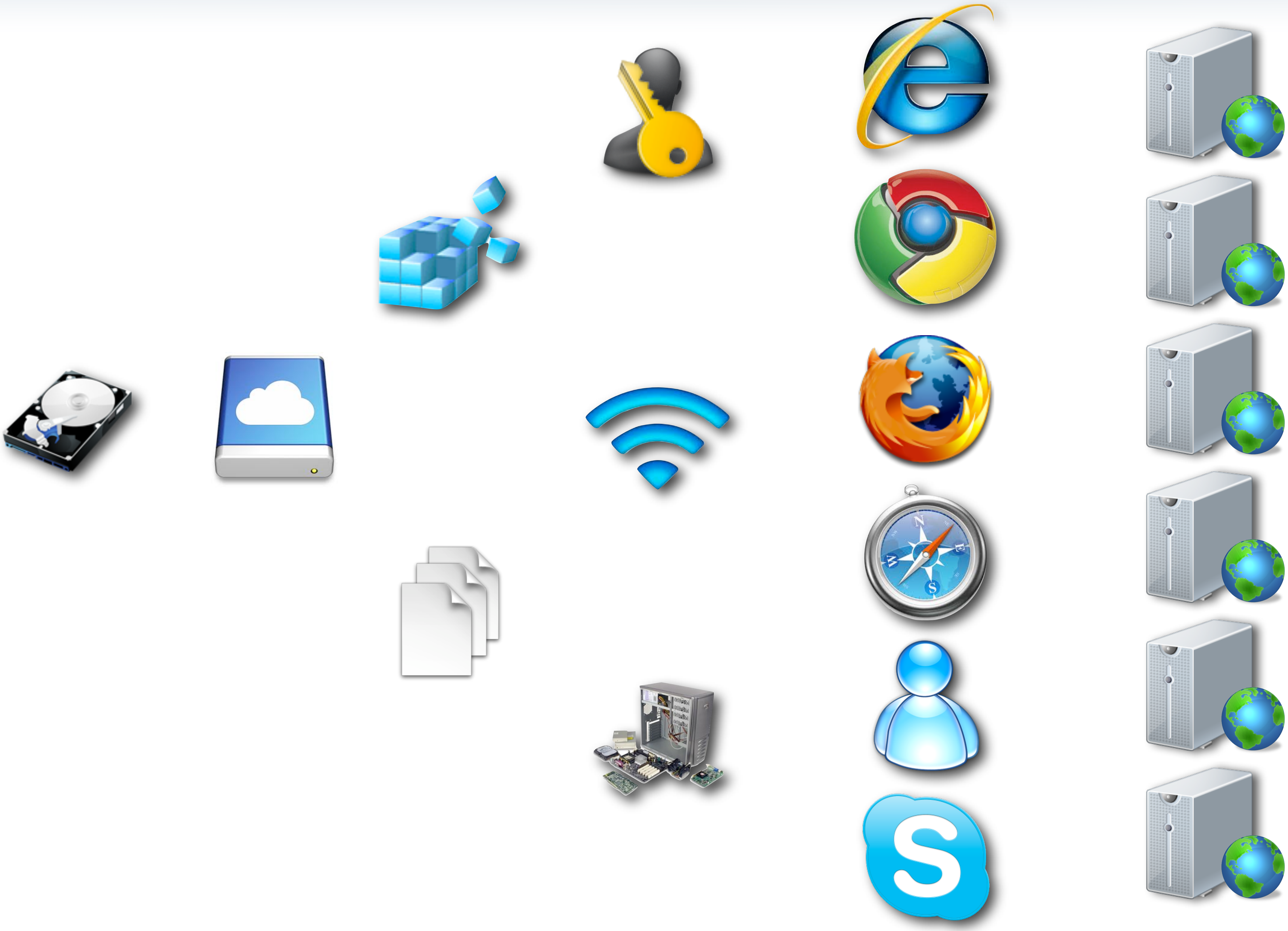
Show you how to bypass the encryption layers and get the data you want

Introducing OWADE

- Dedicated to cloud forensics
- Decrypt / recovers
  - DPAPI secrets
  - Browsers history and websites credentials
  - Instant messaging creds
  - Wifi data
- Free and open-source

http://owade.org

OWADE Overview



Outline

- File base forensics refresher
- The Windows crypto eco-system
- Wifi data and Geo-location
- Recovering browser data
- Recovering instant messaging data
- Acquiring cloud-data
- Demo

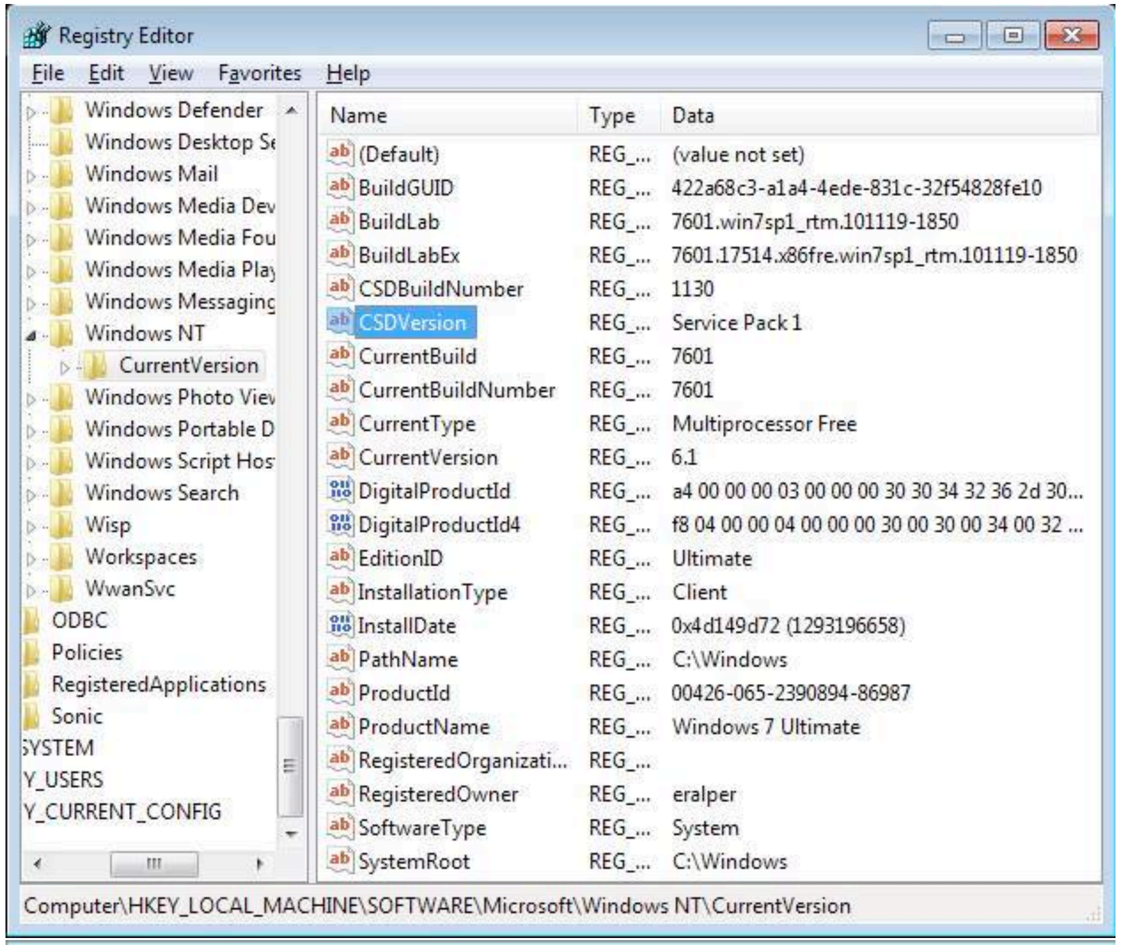
File based forensic refresher

Not all files are born equal

Type of file	how to recover it
Standard	copy
In the trash	undelete utility
Deleted	file carving
Wiped	call the NSA :)

Windows registry

- Hardware information
- Softwares installed with version and serials
- Windows credentials (encrypted)



Windows Defender
Windows Desktop Se
Windows Mail
Windows Media Dev
Windows Media Fou
Windows Media Play
Windows Messaging
Windows NT
CurrentVersion
Windows Photo View
Windows Portable D
Windows Script Hos
Windows Search
Wisp
Workspaces
WwanSvc
ODBC
Policies
RegisteredApplications
Sonic
SYSTEM
Y_USERS
Y_CURRENT_CONFIG

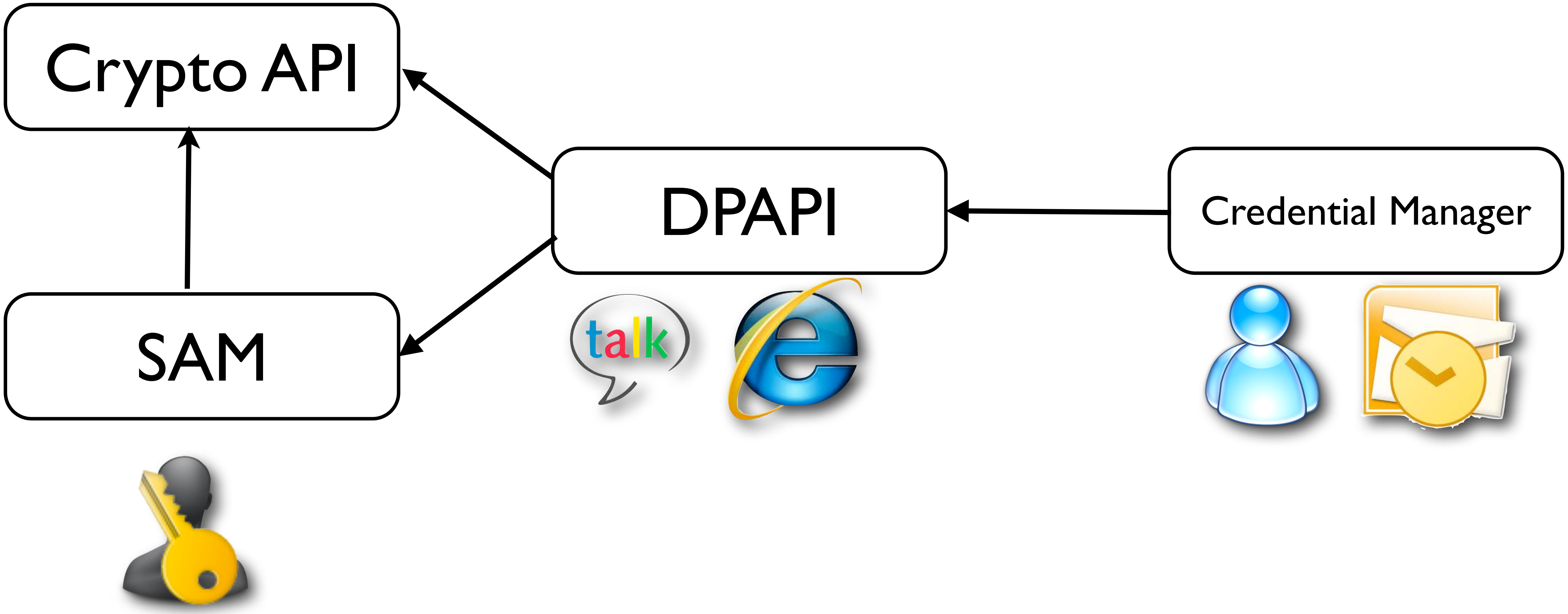
Name	Type	Data
(Default)	REG_...	(value not set)
BuildGUID	REG_...	422a68c3-a1a4-4ede-831c-32f54828fe10
BuildLab	REG_...	7601.win7sp1_rtm.101119-1850
BuildLabEx	REG_...	7601.17514.x86fre.win7sp1_rtm.101119-1850
CSDBuildNumber	REG_...	1130
CSDVersion	REG_...	Service Pack 1
CurrentBuild	REG_...	7601
CurrentBuildNumber	REG_...	7601
CurrentType	REG_...	Multiprocessor Free
CurrentVersion	REG_...	6.1
DigitalProductId	REG_...	a4 00 00 00 03 00 00 00 30 30 34 32 36 2d 30...
DigitalProductId4	REG_...	f8 04 00 00 04 00 00 00 30 00 30 00 34 00 32 ...
EditionID	REG_...	Ultimate
InstallationType	REG_...	Client
InstallDate	REG_...	0x4d149d72 (1293196658)
PathName	REG_...	C:\Windows
ProductId	REG_...	00426-065-2390894-86987
ProductName	REG_...	Windows 7 Ultimate
RegisteredOrganizati...	REG_...	
RegisteredOwner	REG_...	eralper
SoftwareType	REG_...	System
SystemRoot	REG_...	C:\Windows

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

Windows crypto

Many software use Windows Crypto APIs

The Windows crypto eco-system

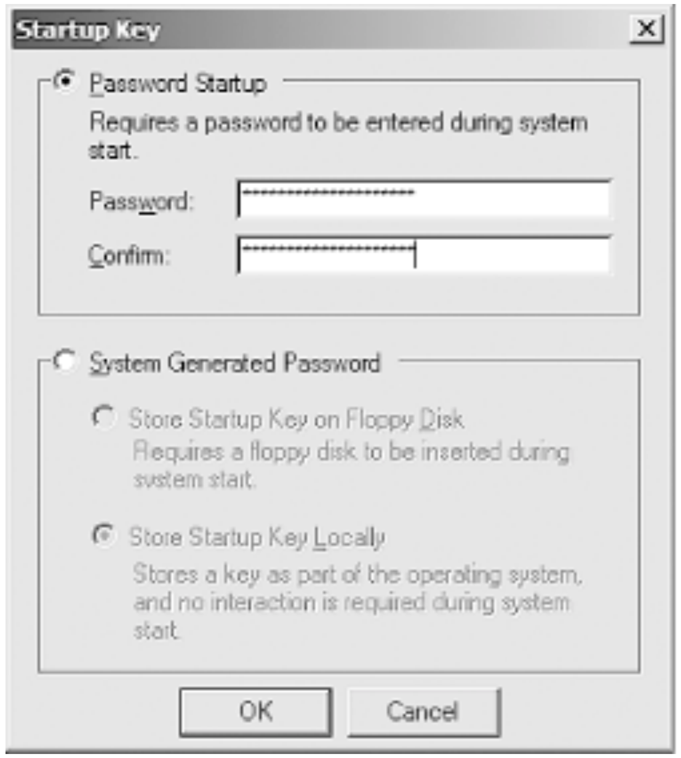


Windows Crypto API

- Basic cryptographic blocks
  - Cipher: 3DES, AES
  - Hash functions: SHA-1 SHA256, HMAC
  - PKI: public keys and certificates (X.509)

The Security Account Manager (SAM)

- Store Windows user credentials
- located in the registry
- Encrypted with the SYSKEY
- Password are hashed



Startup Key

● Password Startup

Requires a password to be entered during system start.

Password: ********************

Confirm: ********************

○ System Generated Password

○ Store Startup Key on Floppy Disk

Requires a floppy disk to be inserted during system start.

● Store Startup Key Locally

Stores a key as part of the operating system, and no interaction is required during system start.

Windows Password Hashing functions

- Two hash functions used
  - LM hash function (NT, 2K, XP, VISTA) weak
  - NTLM (XP, Vista, 7)
- Password are not salted

LM hash weakness

- Use only upper-case
- Hash password in chunk of 7 characters

mypassword →

LMHash(mypassw) +
LMHash(ord)

Password key-space: 69^7 (at most)

Rainbow Tables

- Pre-compute all the possible passwords
- Time-Memory trade-off
- Rainbow tables of all the LM hash are available

How OWADE Works

- Extract Usernames and password hashes
- LM hashes available ?
  - use John/Rainbow tables to get the pass in uppercase
  - use NTLM hashes to find the password cases
- Try to crack the NTLM using John/Rainbow table

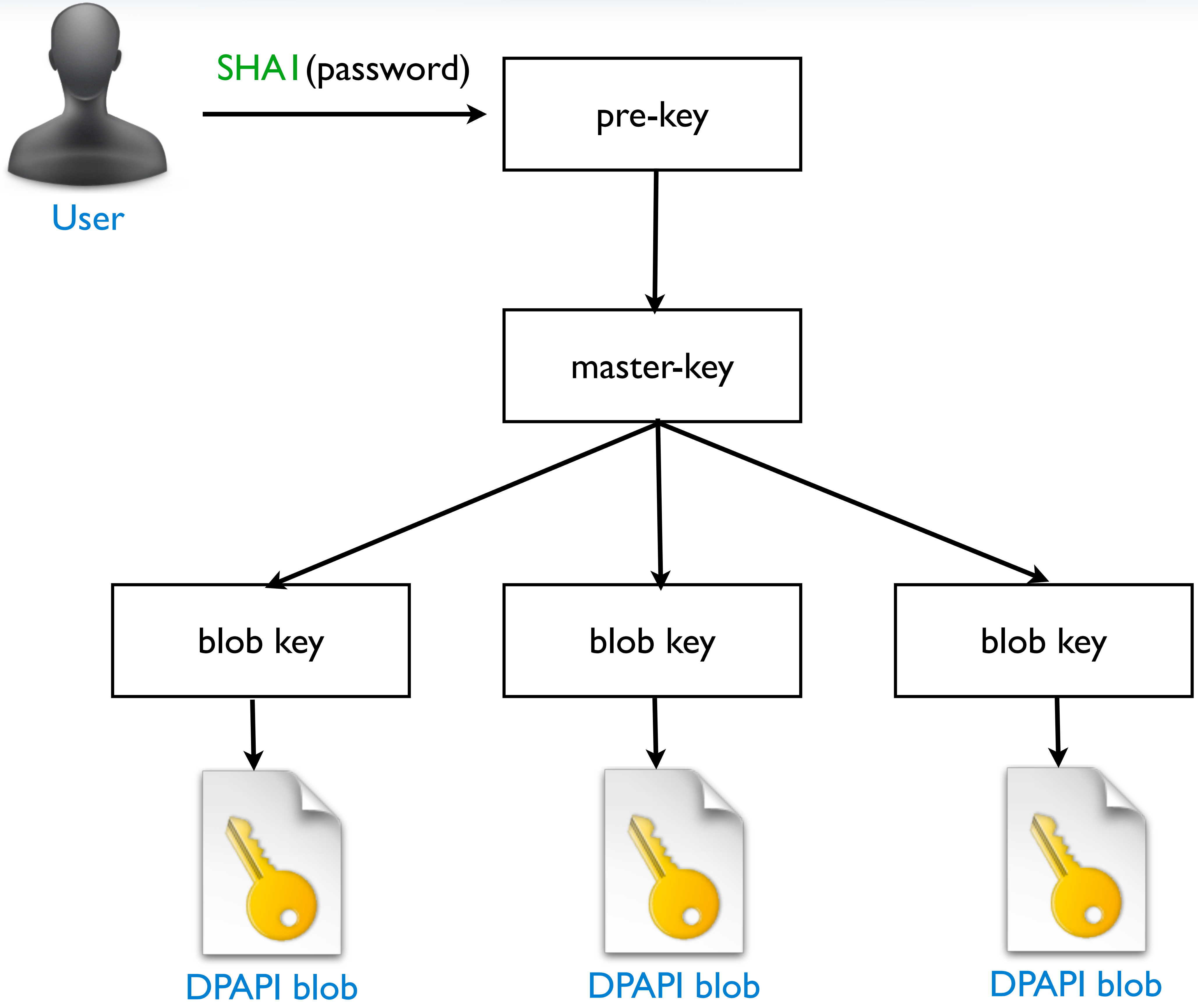
If the password is too strong we can’t recover it

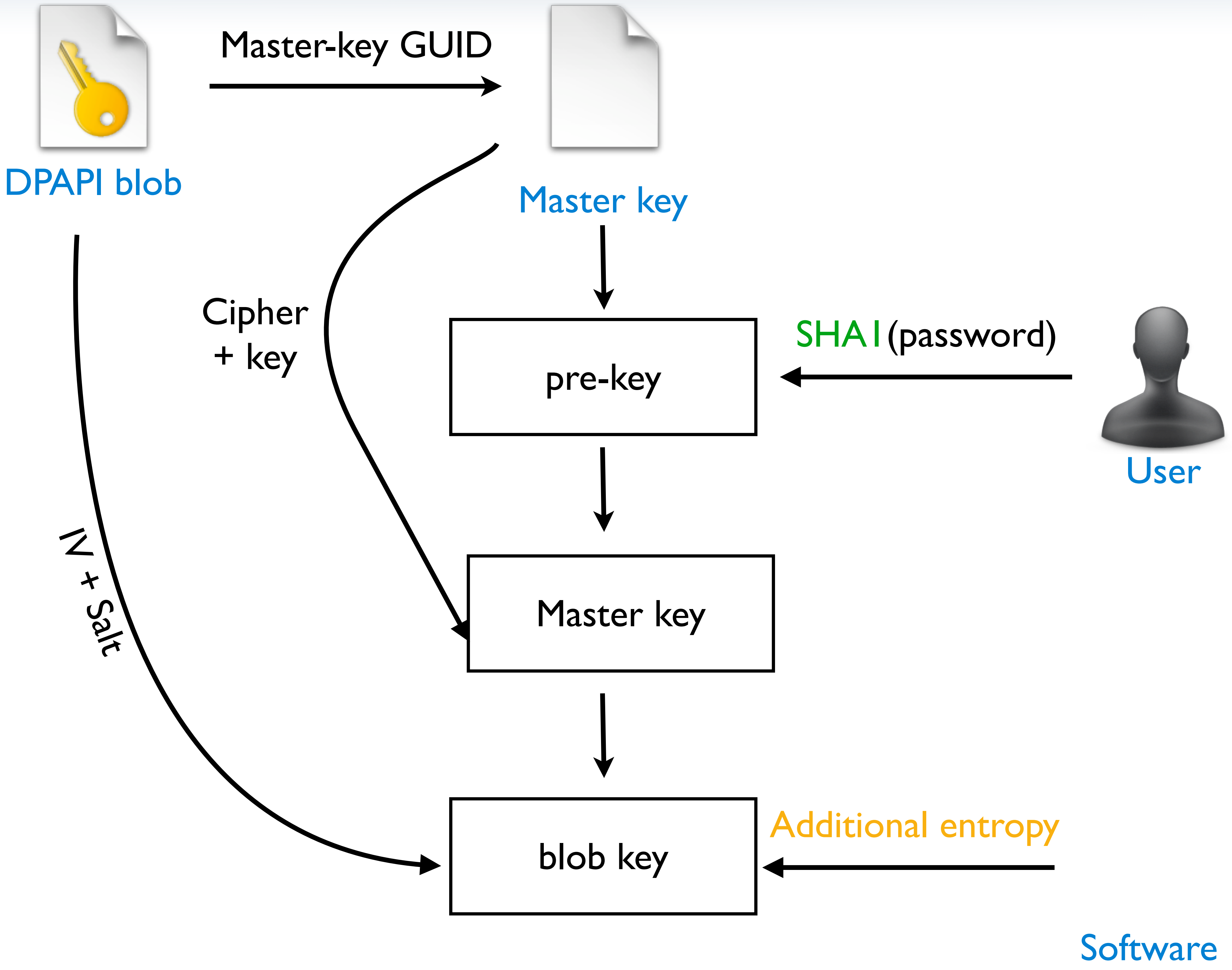
but we can still decrypt DPAPI secret (sometime)

The Data Protection API

- Ensure that encrypted data can’t be decrypted without knowing the user Windows password
- Blackbox crypto API for developers:
  - Encrypt data ⟶ DPAPI blob
  - Decrypt DPAPI blob ⟶ data

DPAPI derivation scheme




Master-key GUID
DPAPI blob
Master key
Cipher
+ key
pre-key
SHA1(password)
User
IV + Salt
Master key
blob key
Additional entropy
Software

Bypassing the user password cracking

- If we can't crack the password we need its SHA1
- This SHA1 is stored in the hibernate file
- OWADE use Moonsol to recover it

Bypassing the user password cracking

- If we can’t crack the password we need its SHA1
- This SHA1 is stored in the hibernate file
- OWADE use Moonsol to recover it

There is an OWADE plugin for that !

DPAPI additional entropy

- Software can supply an additional entropy
  - Act as a “key” (need for decryption)
  - Force us to understand how it is generate for each software
  - Can be used to tie data to a specific machine (i.e Netbios name)

Credential Manager

- Built on top of DPAPI
- Handle transparently the encryption and storage of sensitive data
- Used by Windows, Live Messenger, Remote desktop...

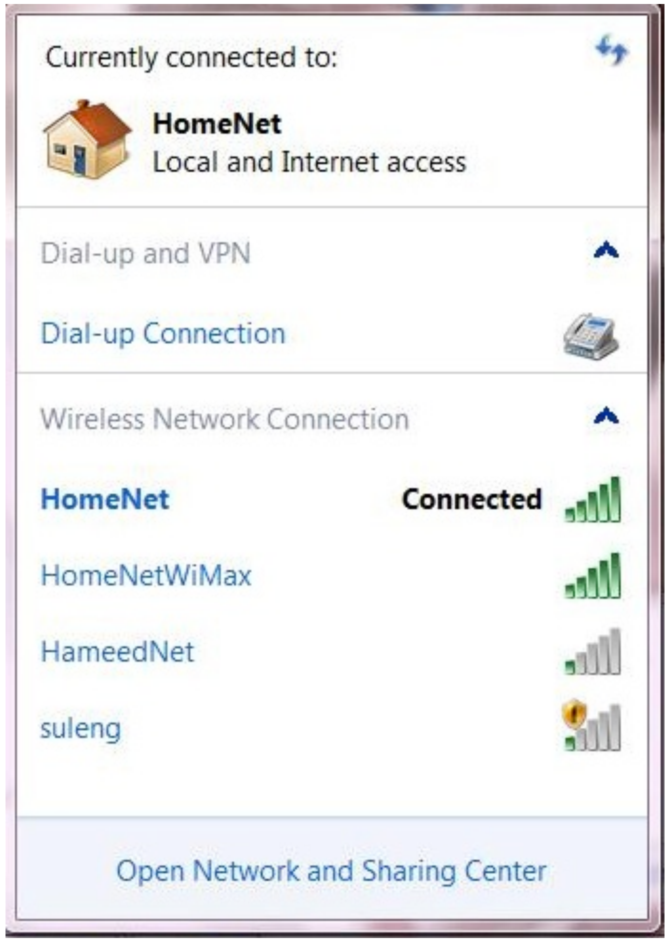
Credstore type of credentials

Type of credential	Encryption	Example of application
Generic password	DPAPI + fixed string	Live messenger HTTP auth (IE)
Domain password	in clear	Netbios
Domain certificate	hash of certificate	Certificate
Domain visible password	DPAPI + fixed string	Remote access .NET passport

WiFi data

Wifi data

- Info stored for each access point
  - Mac address (BSSID)
  - Password (encrypted)
  - Last time of access
- Wifi data are stored in
  - Registry (XP)
  - XML file and Registry (Vista/7)



Currently connected to:

HomeNet
Local and Internet access

Dial-up and VPN

Dial-up Connection

Wireless Network Connection

HomeNet	**Connected**
HomeNetWiMax	
HameedNet	
suleng	

Open Network and Sharing Center

Decrypting WiFi password

- Encrypted with DPAPI
- Access point shared among users
  - Encrypted with the System account
  - But the system account has no password...

What is my DPAPI key ???

Decrypting WiFi password

- Use a LSASecret as DPAPI key
- Recovered with Windows Credentials

Where are you ?

- We've recovered access point keys but where are they ?

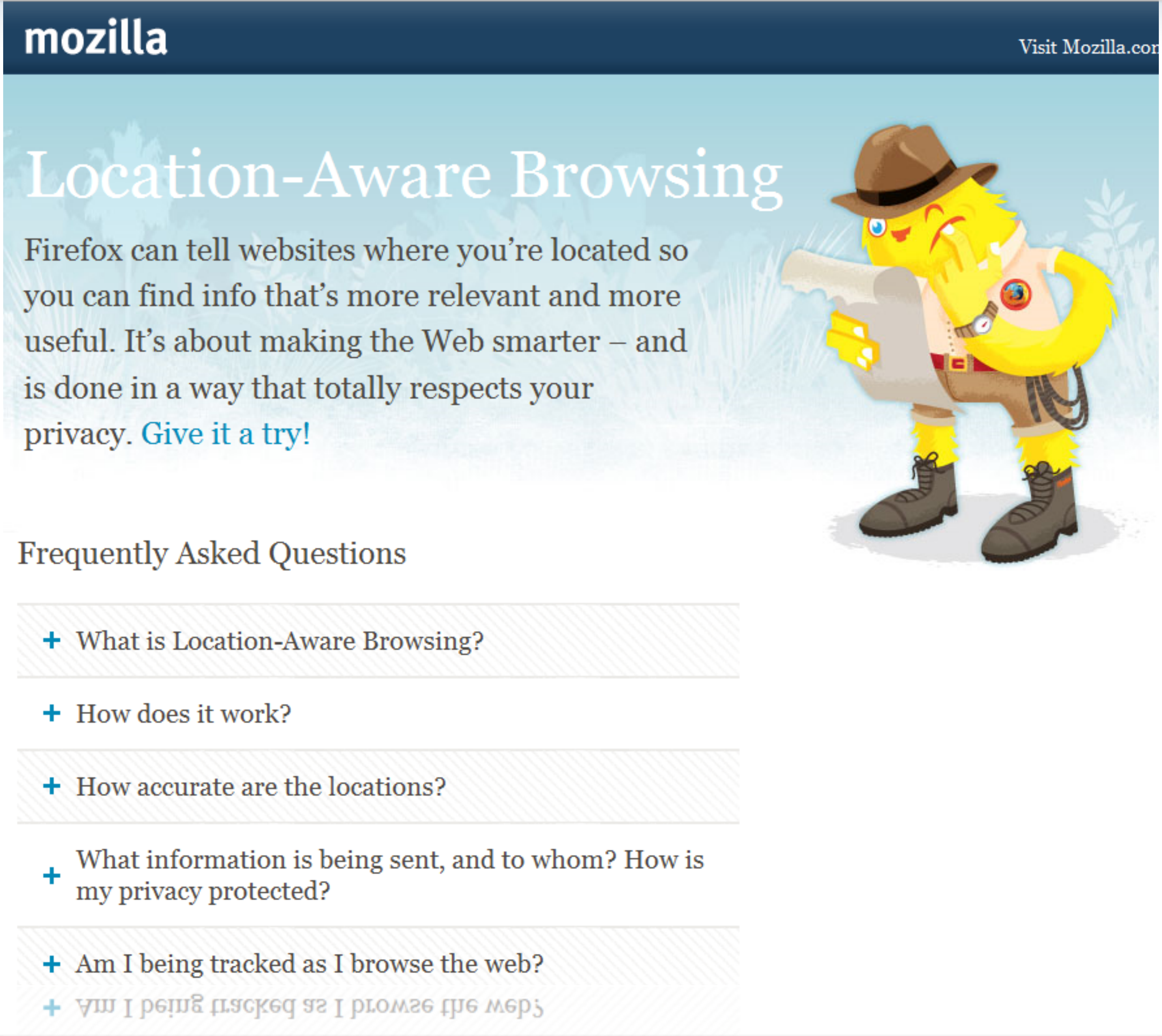
Also found by Sami Kemvar

Where are you ?

- We’ve recovered access point keys but where are they ?

Also found by Sami Kemvar

HTML5 Geo-location protocol



mozilla

Visit Mozilla.cor

Location-Aware Browsing

Firefox can tell websites where you're located so you can find info that's more relevant and more useful. It's about making the Web smarter – and is done in a way that totally respects your privacy. Give it a try!

Frequently Asked Questions

+ What is Location-Aware Browsing?

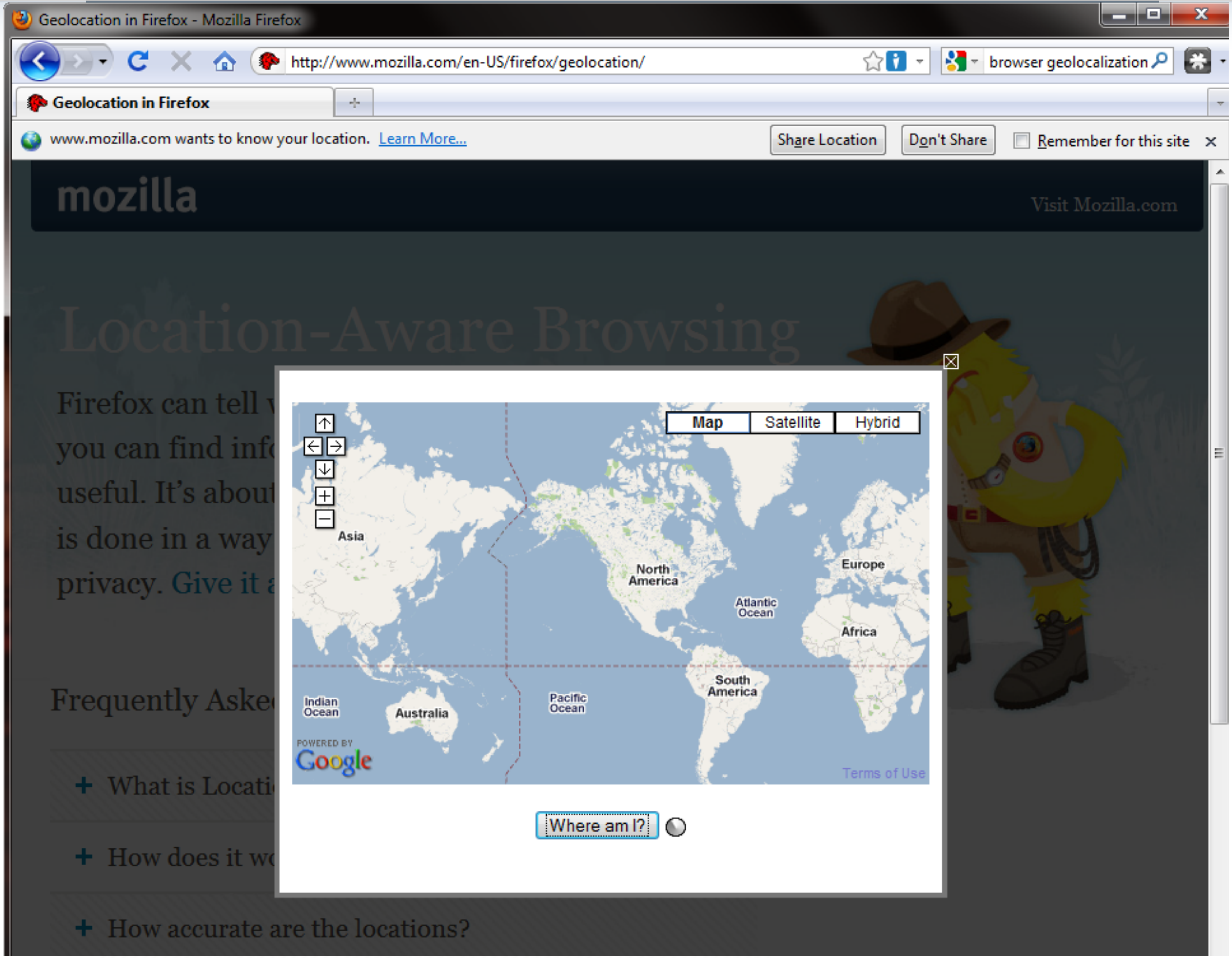
+ How does it work?

+ How accurate are the locations?

+ What information is being sent, and to whom? How is my privacy protected?

+ Am I being tracked as I browse the web?

HTML5 Geo-location protocol



Geolocation in Firefox - Mozilla Firefox

http://www.mozilla.com/en-US/firefox/geolocation/

www.mozilla.com wants to know your location. Learn More...

Location-Aware Browsing

Firefox can tell y
you can find info
useful. It's about
is done in a way
privacy. Give it a

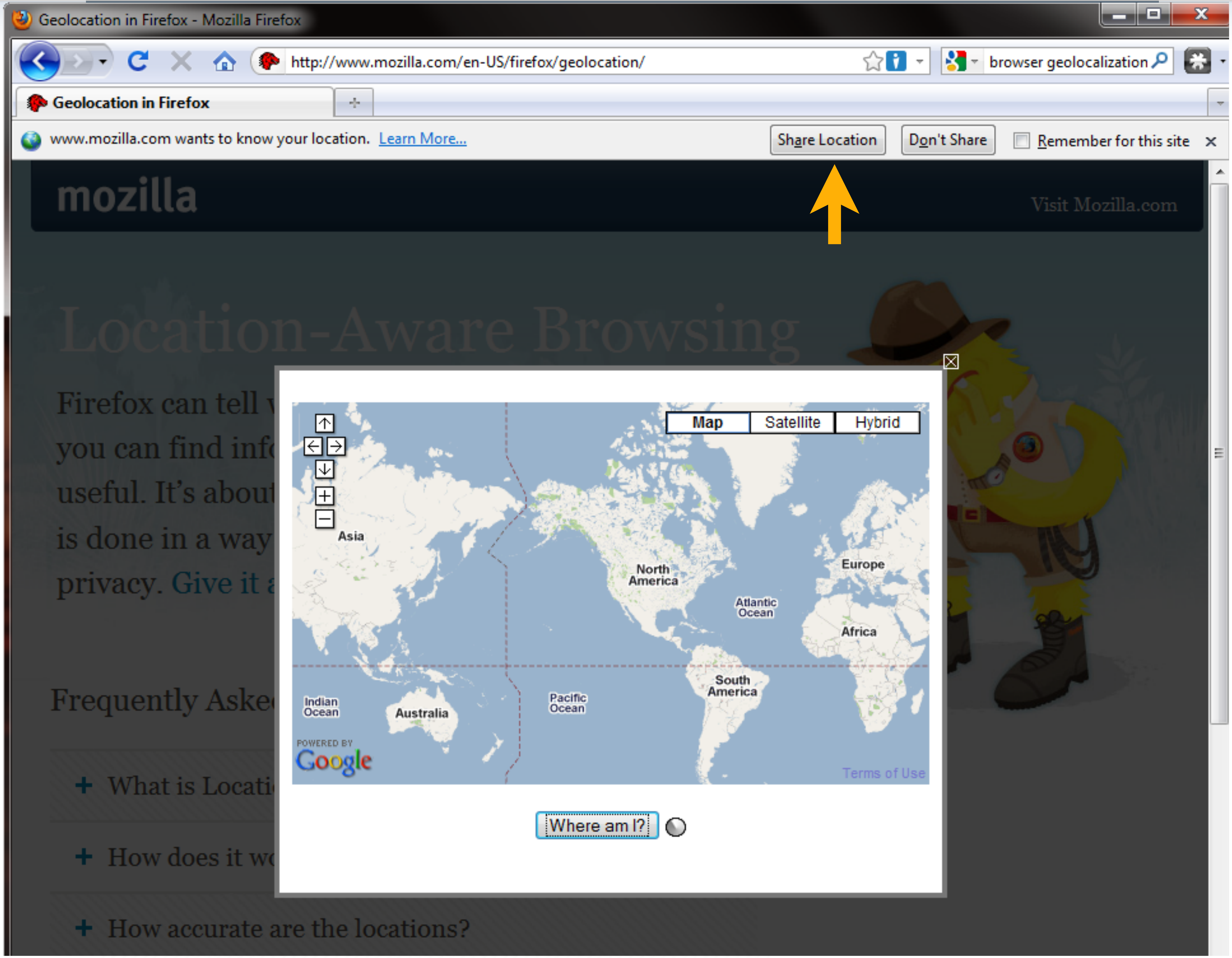
Frequently Aske

+ What is Locati

+ How does it w

+ How accurate are the locations?

HTML5 Geo-location protocol



Geolocation in Firefox - Mozilla Firefox

http://www.mozilla.com/en-US/firefox/geolocation/

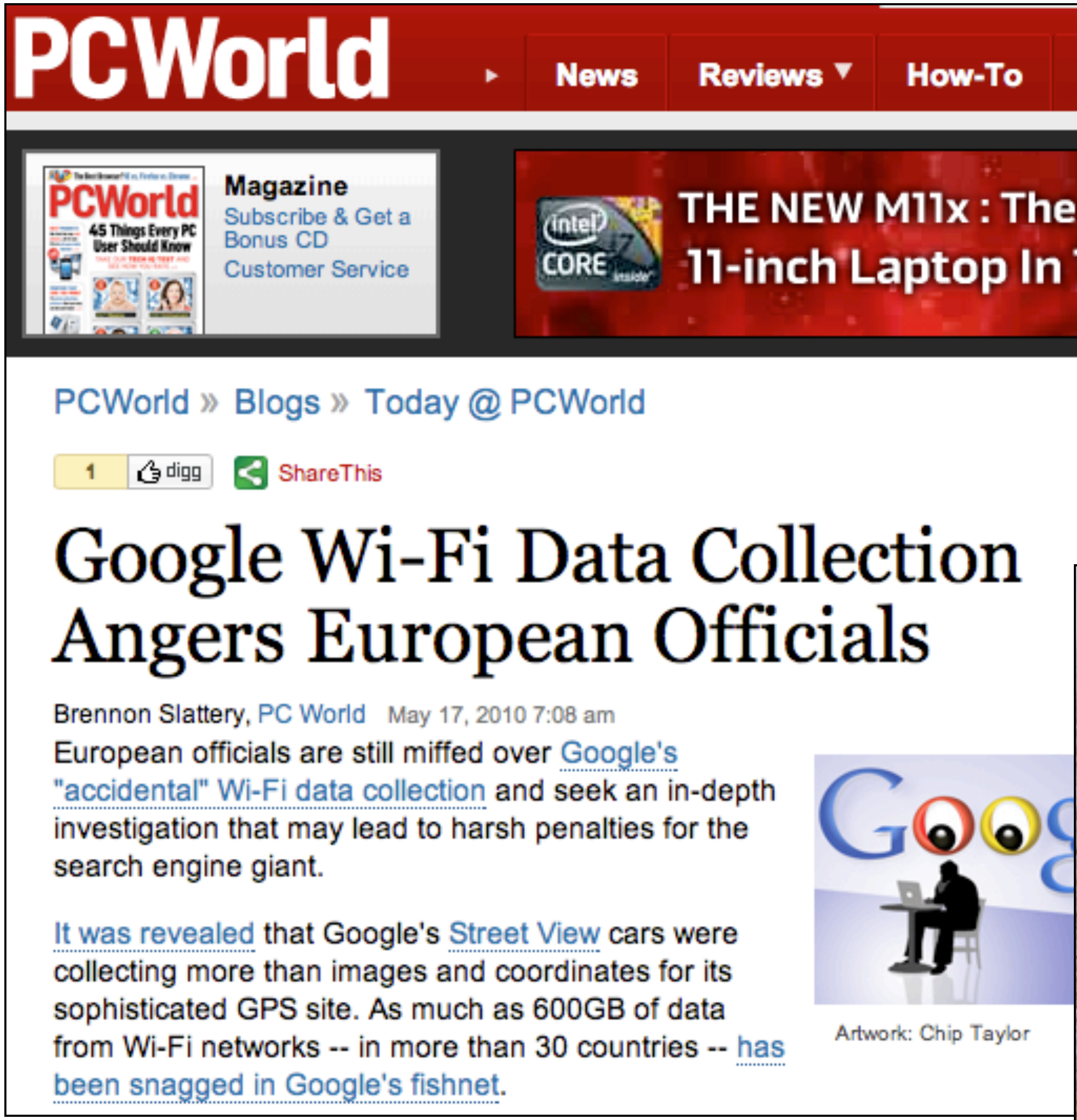
browser geolocalization

Geolocation in Firefox

www.mozilla.com wants to know your location. Learn More...

Share Location | Don't Share | □ Remember for this site

Behind the curtain



PCWorld ▸ News | Reviews ▾ | How-To | Download

Magazine
Subscribe & Get a Bonus CD
Customer Service

PCWorld » Blogs » Today @ PCWorld

1 digg ShareThis

Google Wi-Fi Data Collection Angers European Officials

Brennon Slattery, PC World May 17, 2010 7:08 am

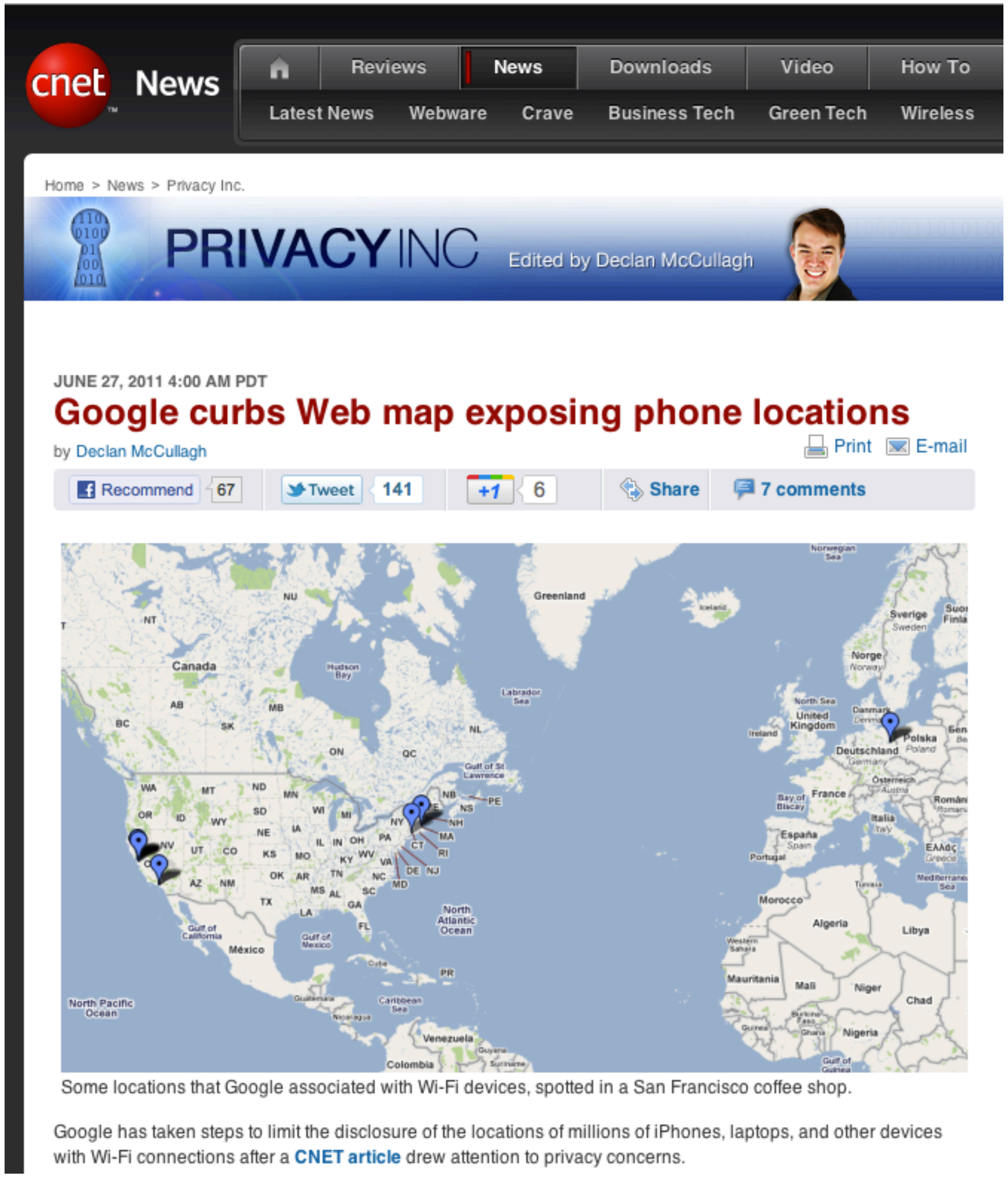
European officials are still miffed over Google's "accidental" Wi-Fi data collection and seek an in-depth investigation that may lead to harsh penalties for the search engine giant.

It was revealed that Google's Street View cars were collecting more than images and coordinates for its sophisticated GPS site. As much as 600GB of data from Wi-Fi networks -- in more than 30 countries -- has been snagged in Google's fishnet.

Artwork: Chip Taylor

Nothing is ever easy

- Google started to restrict queries in June :(
- Fortunately for us there are other API :)



JUNE 27, 2011 4:00 AM PDT

Google curbs Web map exposing phone locations

by Declan McCullagh

Some locations that Google associated with Wi-Fi devices, spotted in a San Francisco coffee shop.

Google has taken steps to limit the disclosure of the locations of millions of iPhones, laptops, and other devices with Wi-Fi connections after a **CNET article** drew attention to privacy concerns.

Geo-location API restrictions

Google™	Requires 2 MAC close from each other
SKYHOOK WIRELESS	The MAC and IP location need to be “close”
Microsoft®	None

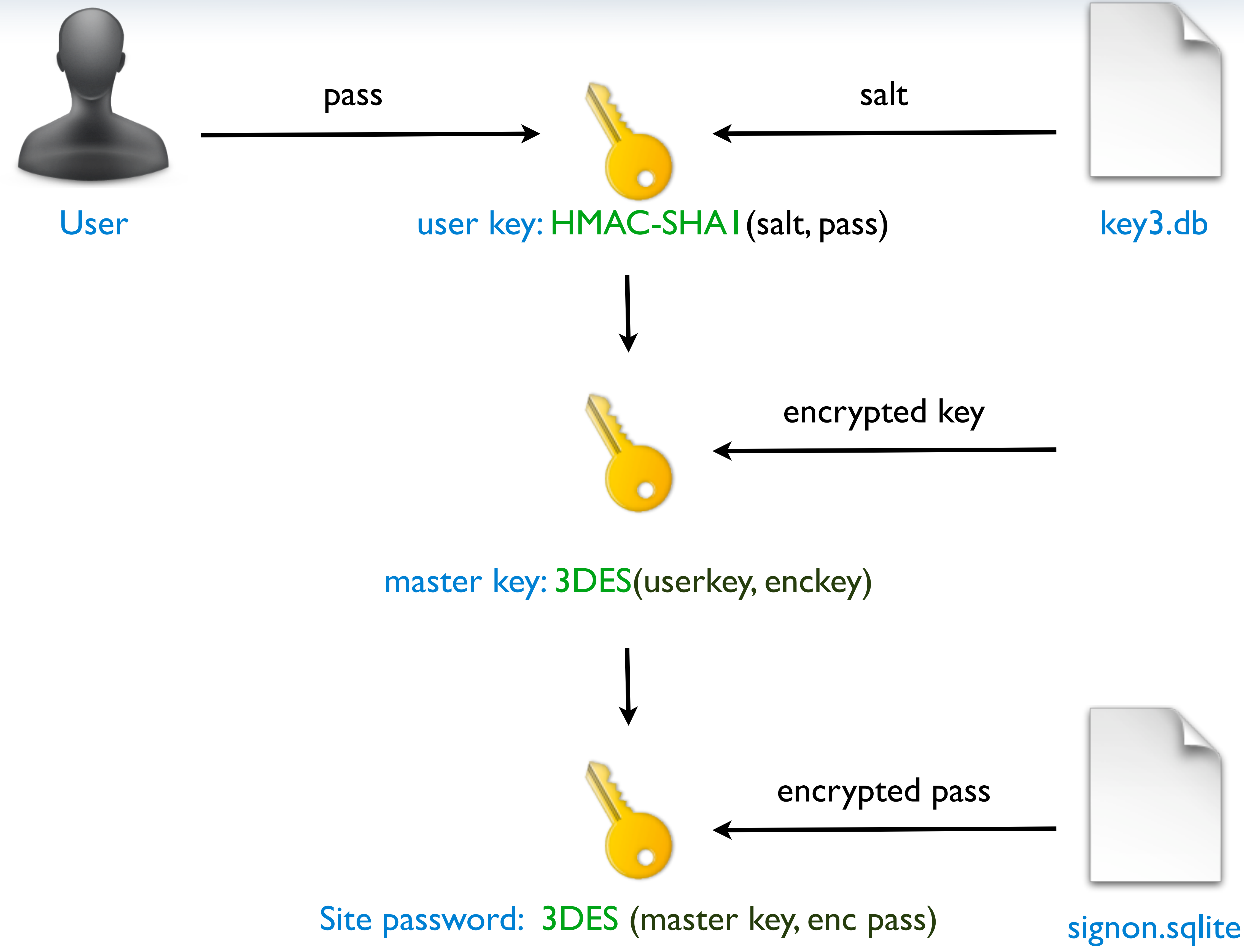
see http://elie.im/blog/ for more information

Browsers

Firefox > 3.4

- Passwords
  - location: signons.sqlite
  - encryption: 3DES + Master password
- History
  - URLs: places.sqlite
  - Forms fields: formhistory.sqlite

Decrypting Firefox password



pass

salt

User

user key: HMAC-SHA1(salt, pass)

key3.db

encrypted key

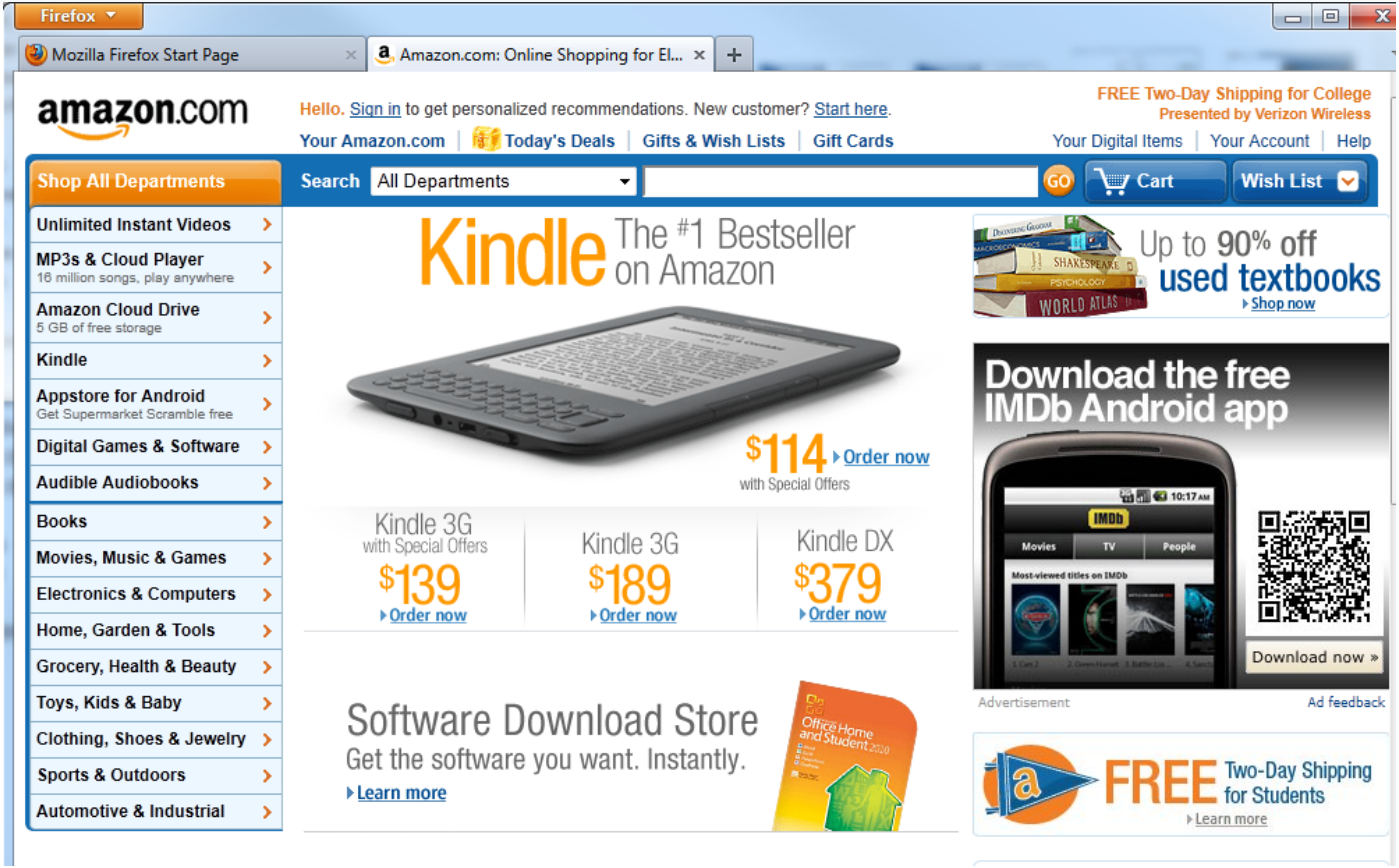
master key: 3DES(userkey, enckey)

encrypted pass

Site password: 3DES (master key, enc pass)

signon.sqlite

Shopping at Amazon ?



Firefox
Mozilla Firefox Start Page
Amazon.com: Online Shopping for El...
amazon.com

Hello. Sign in to get personalized recommendations. New customer? Start here.

FREE Two-Day Shipping for College
Presented by Verizon Wireless

Your Amazon.com | Today's Deals | Gifts & Wish Lists | Gift Cards

Your Digital Items | Your Account | Help

Shop All Departments

Search All Departments GO Cart Wish List

- Unlimited Instant Videos
- MP3s & Cloud Player
  16 million songs, play anywhere
- Amazon Cloud Drive
  5 GB of free storage
- Kindle
- Appstore for Android
  Get Supermarket Scramble free
- Digital Games & Software
- Audible Audiobooks
- Books
- Movies, Music & Games
- Electronics & Computers
- Home, Garden & Tools
- Grocery, Health & Beauty
- Toys, Kids & Baby
- Clothing, Shoes & Jewelry
- Sports & Outdoors
- Automotive & Industrial

Kindle The #1 Bestseller on Amazon

$114 Order now
with Special Offers

Kindle 3G with Special Offers	Kindle 3G	Kindle DX
$139	$189	$379
Order now	Order now	Order now

Software Download Store
Get the software you want. Instantly.
Learn more

Up to 90% off used textbooks
Shop now

Download the free IMDb Android app

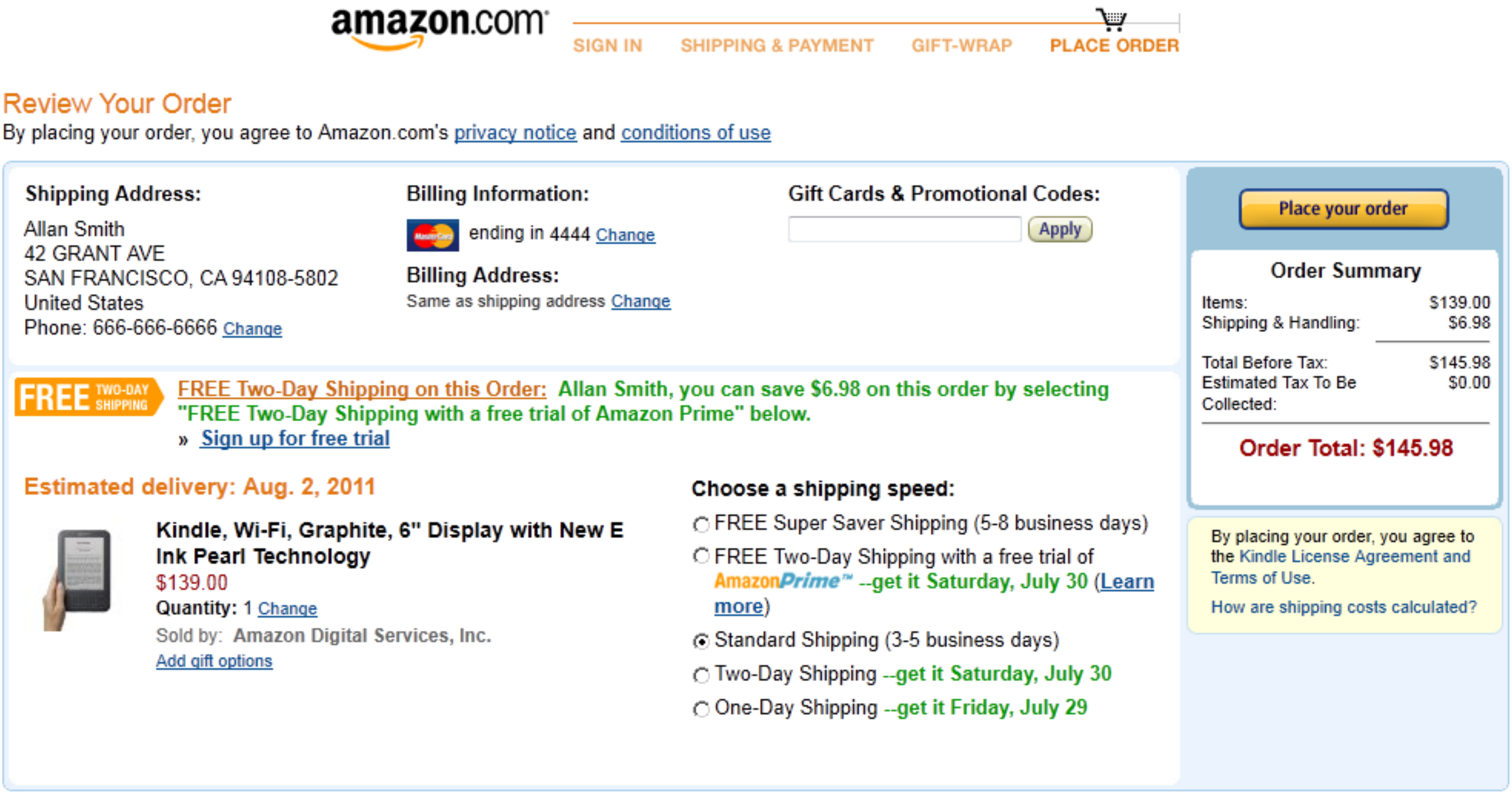
Download now »

Advertisement

Ad feedback

FREE Two-Day Shipping for Students
Learn more

How about a nice kindle ?



Review Your Order

By placing your order, you agree to Amazon.com's privacy notice and conditions of use

Shipping Address:

Allan Smith
42 GRANT AVE
SAN FRANCISCO, CA 94108-5802
United States
Phone: 666-666-6666 Change

Billing Information:

ending in 4444 Change

Billing Address:

Same as shipping address Change

Gift Cards & Promotional Codes:

Apply

FREE TWO-DAY SHIPPING FREE Two-Day Shipping on this Order: Allan Smith, you can save $6.98 on this order by selecting "FREE Two-Day Shipping with a free trial of Amazon Prime" below.

» Sign up for free trial

Estimated delivery: Aug. 2, 2011

Kindle, Wi-Fi, Graphite, 6" Display with New E Ink Pearl Technology
$139.00
Quantity: 1 Change
Sold by: Amazon Digital Services, Inc.
Add gift options

Choose a shipping speed:

○ FREE Super Saver Shipping (5-8 business days)
○ FREE Two-Day Shipping with a free trial of AmazonPrime™ --get it Saturday, July 30 (Learn more)
● Standard Shipping (3-5 business days)
○ Two-Day Shipping --get it Saturday, July 30
○ One-Day Shipping --get it Friday, July 29

Place your order

Order Summary

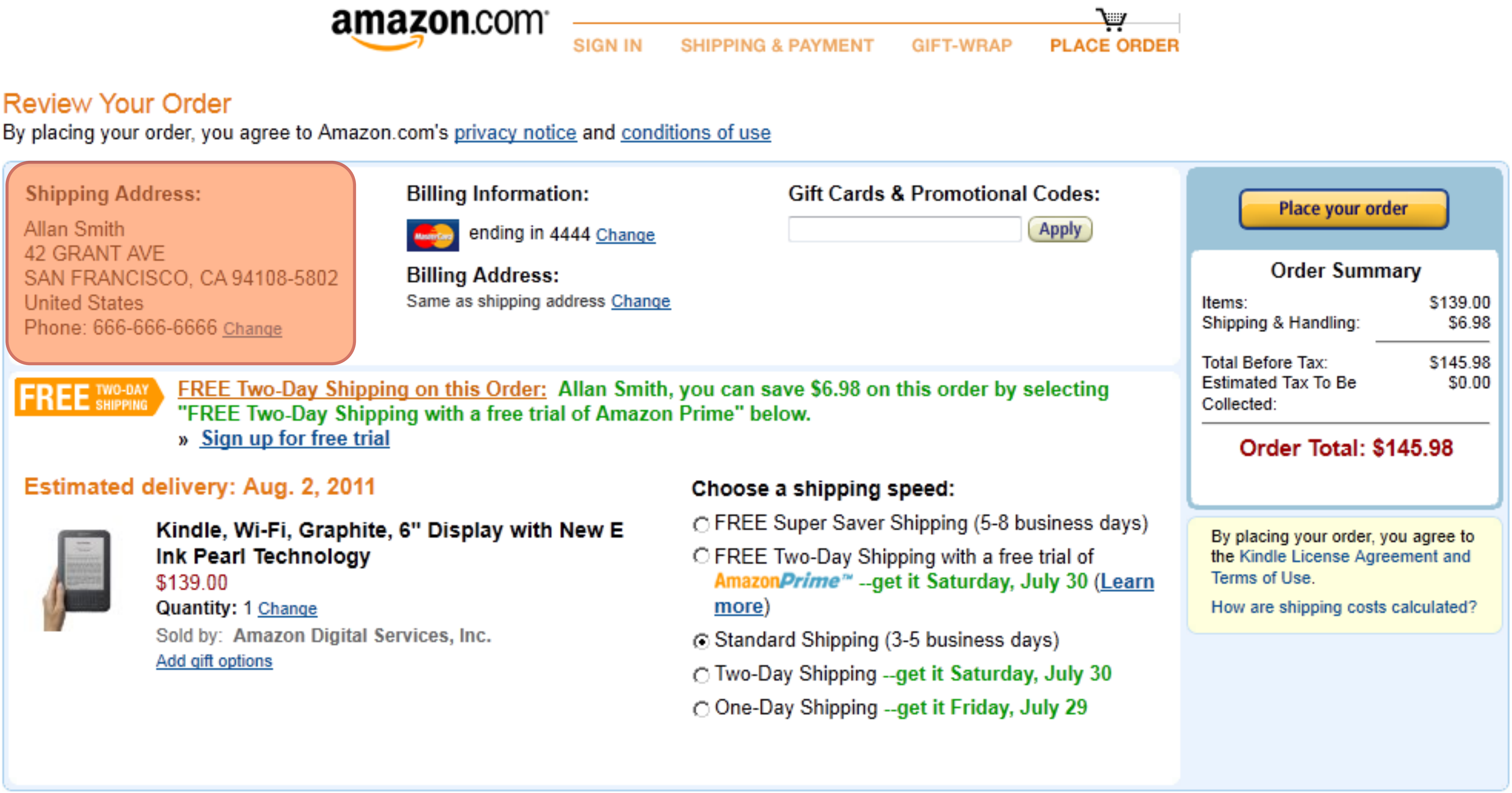
Items:	$139.00
Shipping & Handling:	$6.98
Total Before Tax:	$145.98
Estimated Tax To Be Collected:	$0.00

Order Total: $145.98

By placing your order, you agree to the Kindle License Agreement and Terms of Use.

How are shipping costs calculated?

How about a nice kindle ?



Review Your Order

By placing your order, you agree to Amazon.com's privacy notice and conditions of use

Shipping Address:

Allan Smith
42 GRANT AVE
SAN FRANCISCO, CA 94108-5802
United States
Phone: 666-666-6666 Change

Billing Information:

ending in 4444 Change

Billing Address:

Same as shipping address Change

Gift Cards & Promotional Codes:

Order Summary

Items:	$139.00
Shipping & Handling:	$6.98
Total Before Tax:	$145.98
Estimated Tax To Be Collected:	$0.00

Order Total: $145.98

FREE Two-Day Shipping on this Order: Allan Smith, you can save $6.98 on this order by selecting "FREE Two-Day Shipping with a free trial of Amazon Prime" below.

» Sign up for free trial

Estimated delivery: Aug. 2, 2011

Kindle, Wi-Fi, Graphite, 6" Display with New E Ink Pearl Technology
$139.00
Quantity: 1 Change
Sold by: Amazon Digital Services, Inc.
Add gift options

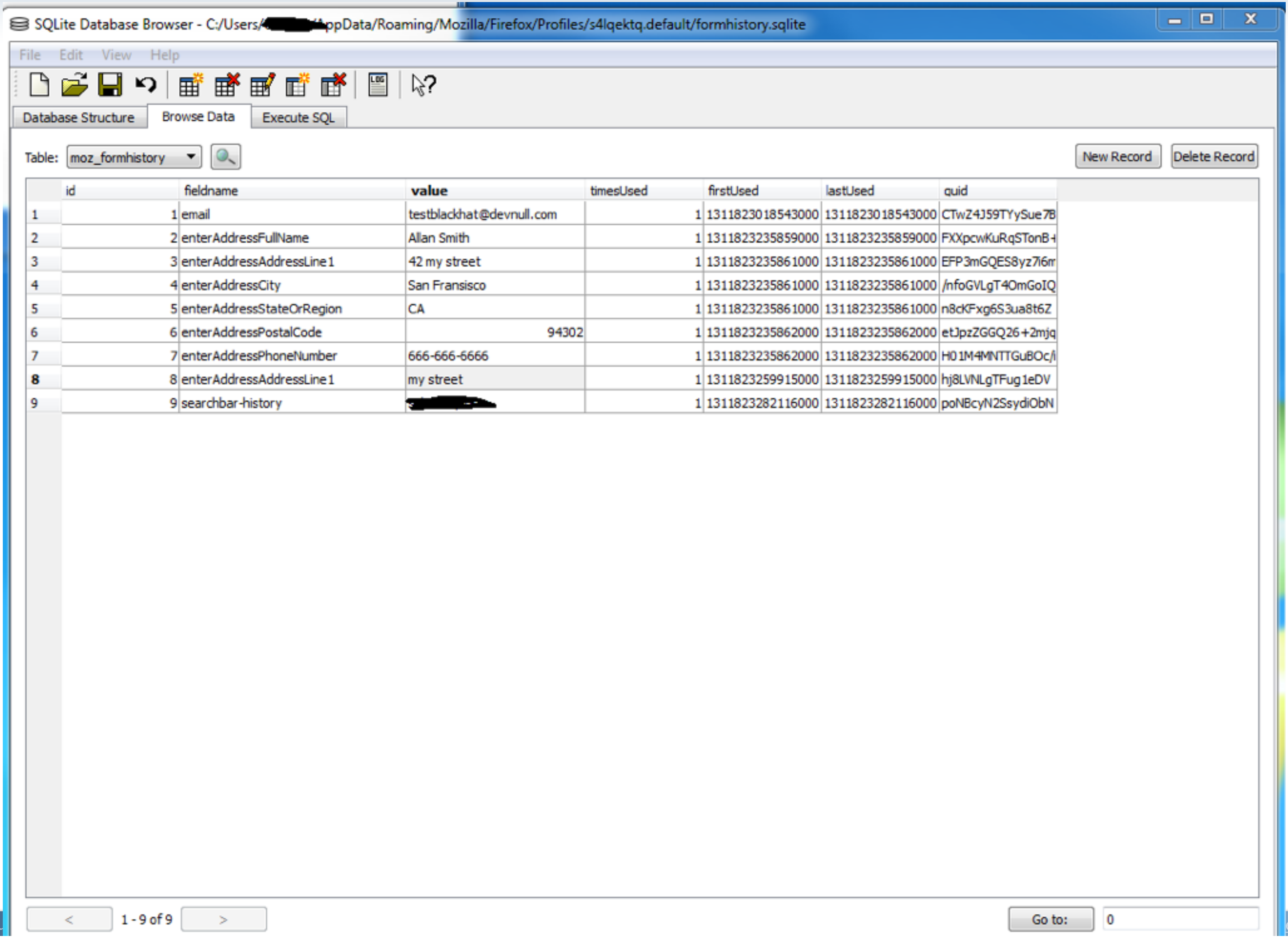
Choose a shipping speed:

○ FREE Super Saver Shipping (5-8 business days)
○ FREE Two-Day Shipping with a free trial of AmazonPrime™ --get it Saturday, July 30 (Learn more)
● Standard Shipping (3-5 business days)
○ Two-Day Shipping --get it Saturday, July 30
○ One-Day Shipping --get it Friday, July 29

By placing your order, you agree to the Kindle License Agreement and Terms of Use.

How are shipping costs calculated?

Every form field is recorded



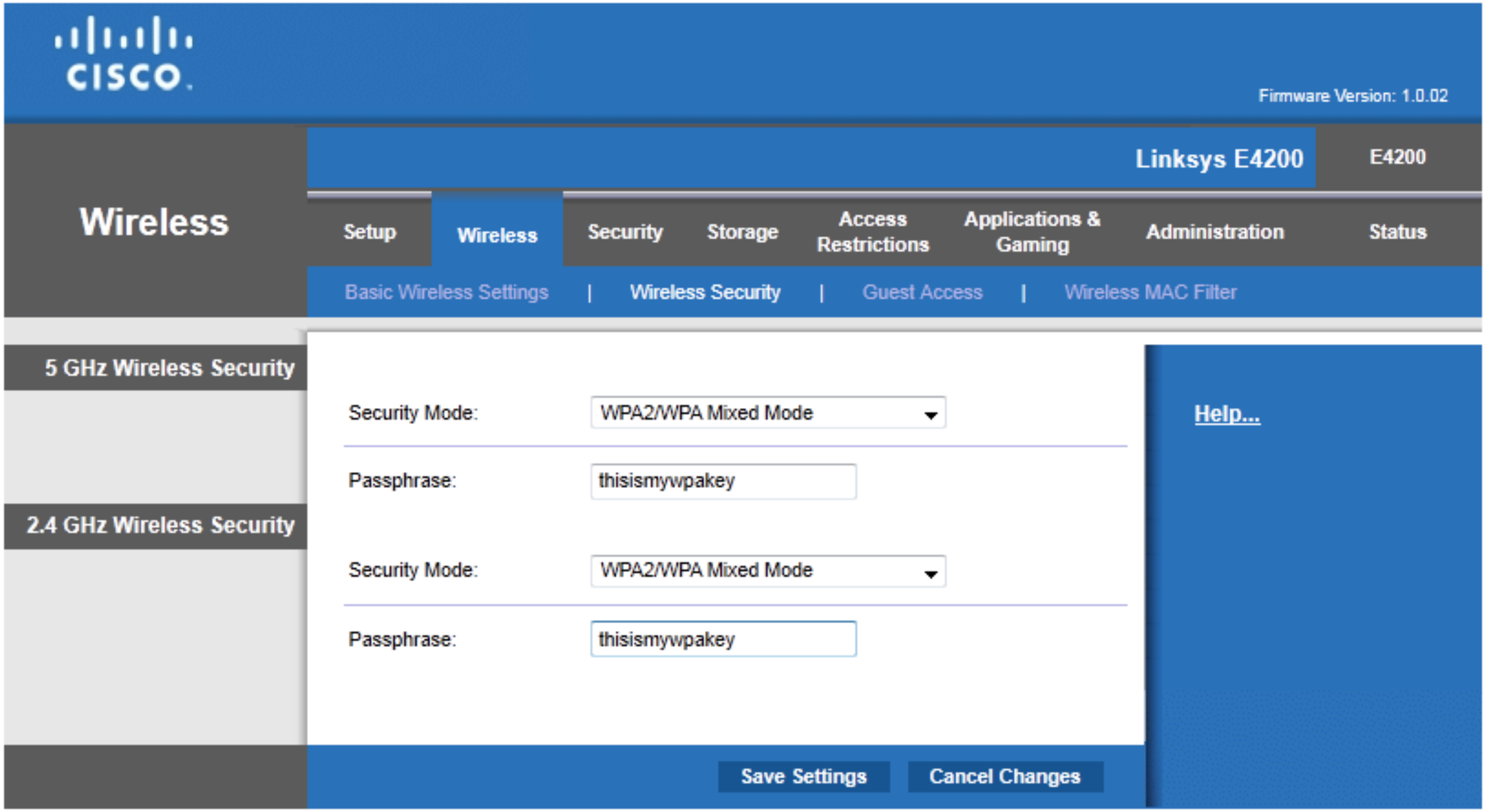
SQLite Database Browser - C:/Users/[redacted]ppData/Roaming/Mozilla/Firefox/Profiles/s4lqektq.default/formhistory.sqlite

Table: moz_formhistory

	id	fieldname	value	timesUsed	firstUsed	lastUsed	quid
1	1	email	testblackhat@devnull.com	1	1311823018543000	1311823018543000	CTwZ4J59TYySue7B
2	2	enterAddressFullName	Allan Smith	1	1311823235859000	1311823235859000	FXXpcwKuRqSTonB+
3	3	enterAddressAddressLine1	42 my street	1	1311823235861000	1311823235861000	EFP3mGQES8yz7i6m
4	4	enterAddressCity	San Fransisco	1	1311823235861000	1311823235861000	/nfoGVLgT4OmGoIQ
5	5	enterAddressStateOrRegion	CA	1	1311823235861000	1311823235861000	n8cKFxg6S3ua8t6Z
6	6	enterAddressPostalCode	94302	1	1311823235862000	1311823235862000	etJpzZGGQ26+2mjq
7	7	enterAddressPhoneNumber	666-666-6666	1	1311823235862000	1311823235862000	H01M4MNTTGuBOc/i
8	8	enterAddressAddressLine1	my street	1	1311823259915000	1311823259915000	hj8LVNLgTFug1eDV
9	9	searchbar-history	[redacted]	1	1311823282116000	1311823282116000	poNBcyN2SsydiObN

Go to: 0

Configuring a Linksys ?



5 GHz Wireless Security

Security Mode: WPA2/WPA Mixed Mode

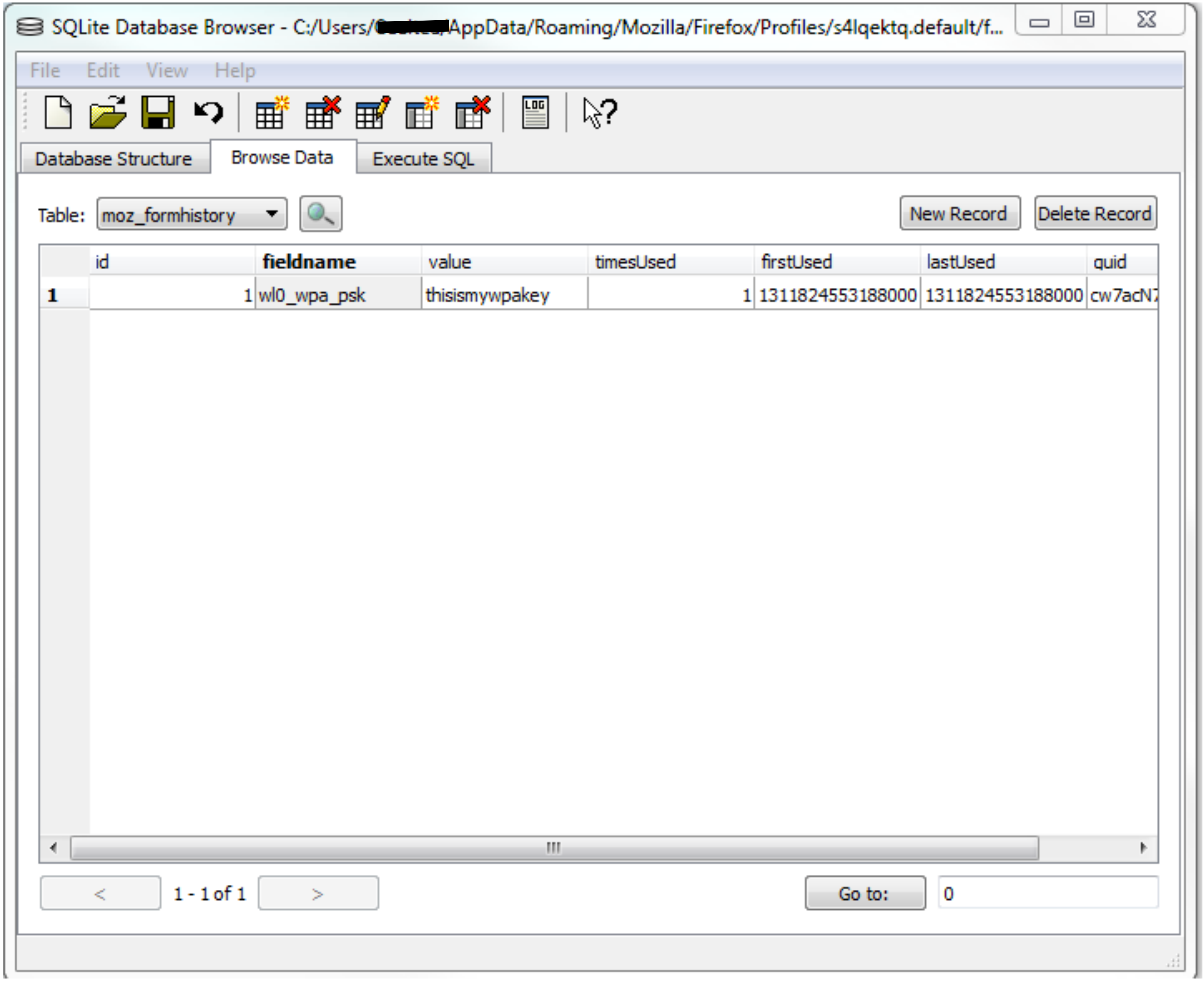
Passphrase: thisismywpakey

2.4 GHz Wireless Security

Security Mode: WPA2/WPA Mixed Mode

Passphrase: thisismywpakey

Again the key is recorded



SQLite Database Browser - C:/Users/[redacted]AppData/Roaming/Mozilla/Firefox/Profiles/s4lqektq.default/f...

Table: moz_formhistory

	id	fieldname	value	timesUsed	firstUsed	lastUsed	guid
1	1	wl0_wpa_psk	thisismywpakey	1	1311824553188000	1311824553188000	cw7acN7

Form history leak a lot of information

- Shipping address
- Wifi key
- Credit card information
- Email
- Search history

Preventing field recording

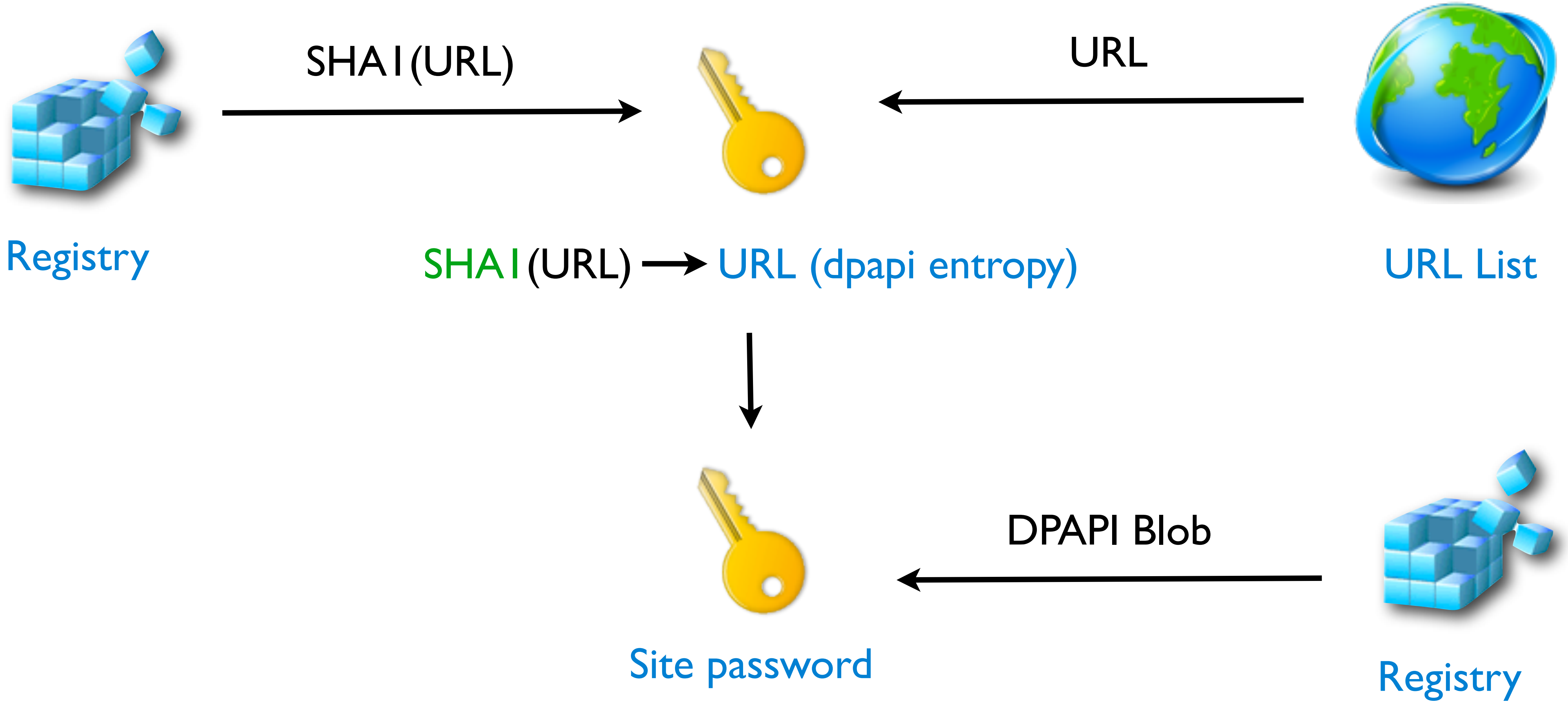
To tell the browser to not record a field use the tag

autocomplete=”off”

Internet Explorer

- Passwords
  - location: registry
  - encryption: DPAPI + URL as salt
- History
  - URLs: Index.dat
  - Forms fields:

Decrypting Internet Explorer passwords



SHA1(URL)

URL

Registry

SHA1(URL) ⟶ URL (dpapi entropy)

URL List

DPAPI Blob

Site password

Registry

Chrome

- Passwords
  - location: login data (sqlite)
  - encryption: DPAPI
- History
  - URLs: History (sqlite)
  - Forms fields: Web data (sqlite)

Safari

- Passwords
  - location: keychain.plist
  - encryption: DPAPI + fixed string as entropy
  - History
  - URLs: History.plist (Property list format)
  - Forms fields: Form Value.plist

Browsers takeaway

- Internet Explorer is the most secure.
  - If you don’t know the URL you can’t recover the pass
- Firefox is the worst
  - Passwords encryption not tied to the Windows pass
  - Login are encrypted in signons.sqlite not in formhistory.sqlite

Private mode

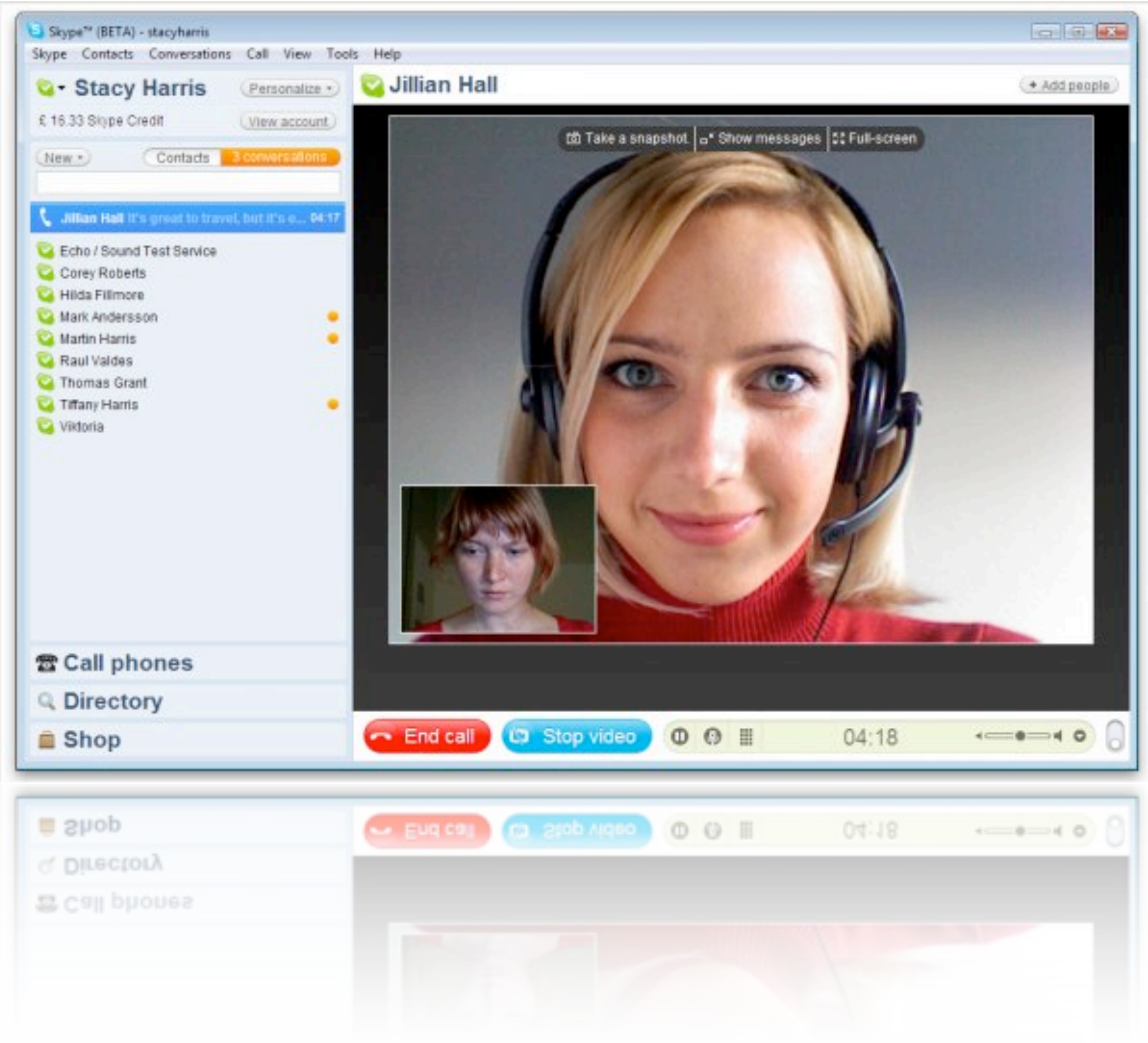
- Most bugs are fixed
- Requires to be creative
  - SSL OCSP requests
  - File carving
- Potential techniques
  - Analyze the hibernate file

See: http://ly.tl/p16 for more information on private mode

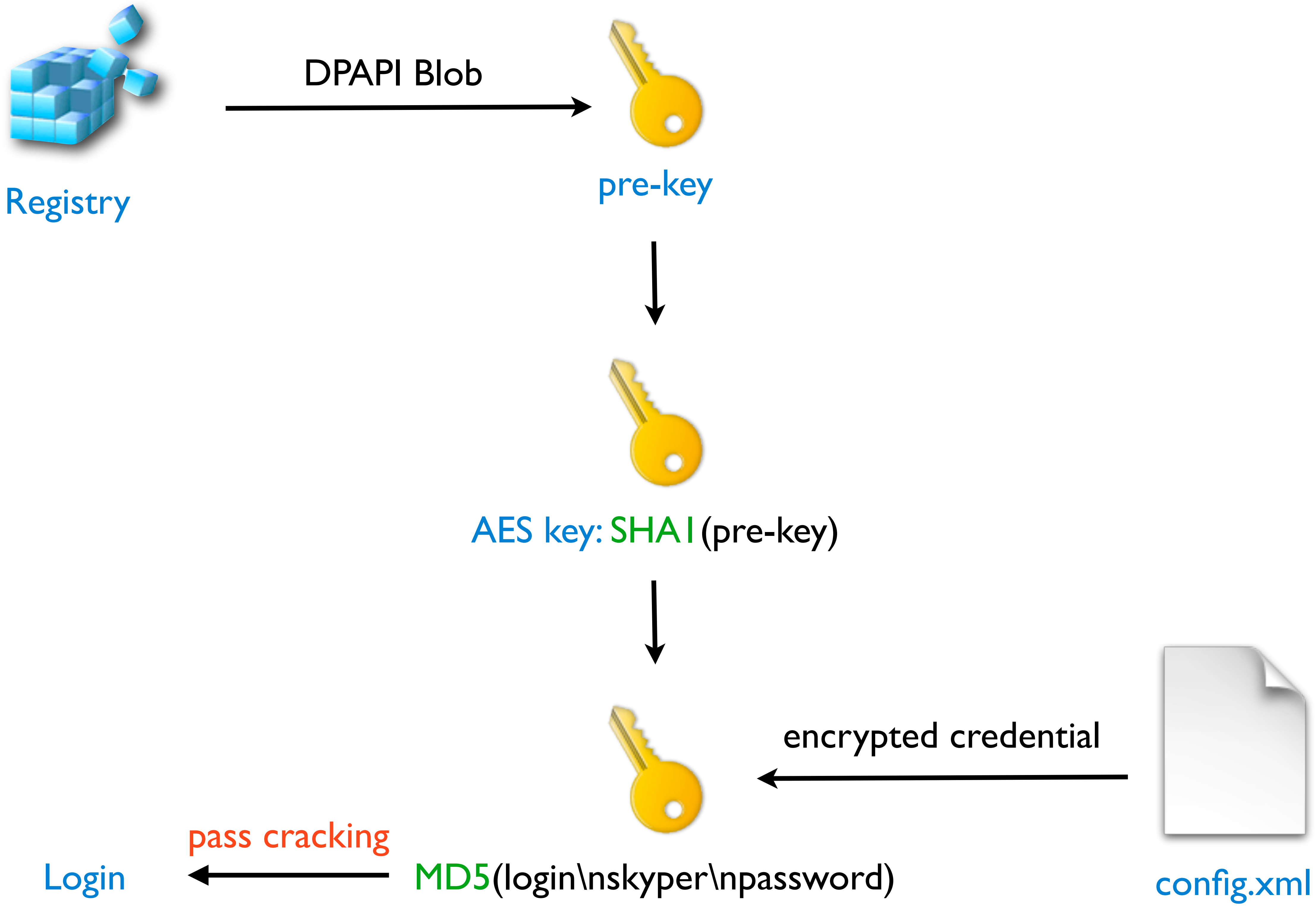
Instant messaging

Skype

- Encryption
  custom
- Difficulty
  extreme
- Location
  registry + config.xml



Decrypting Skype passwords



DPAPI Blob

Registry

pre-key

AES key: SHA1(pre-key)

encrypted credential

config.xml

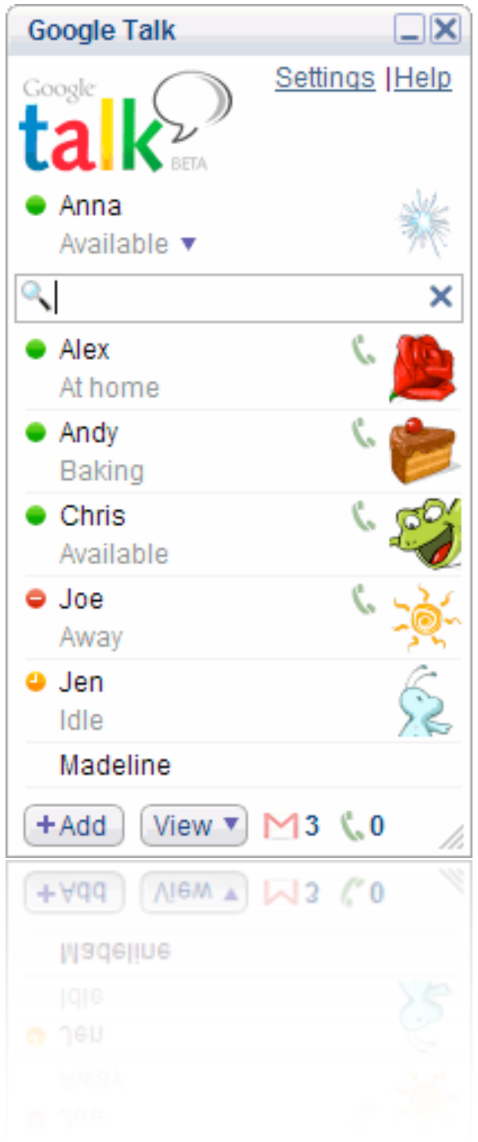
pass cracking

Login

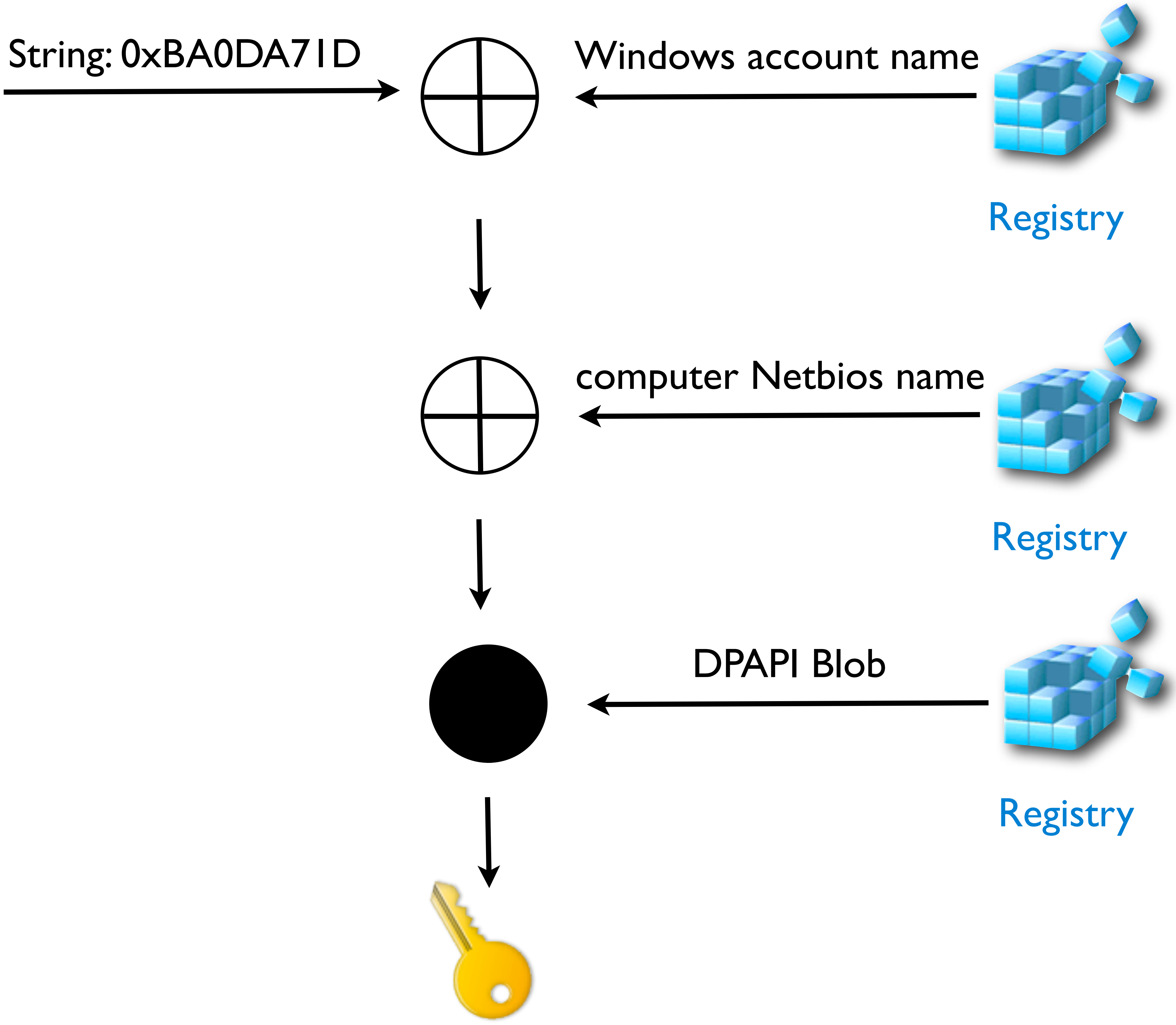
MD5(login\nskyper\npassword)

Google Talk

- Encryption
  DPAPI + custom (salt)
- Difficulty
  Hard
- Location
  registry

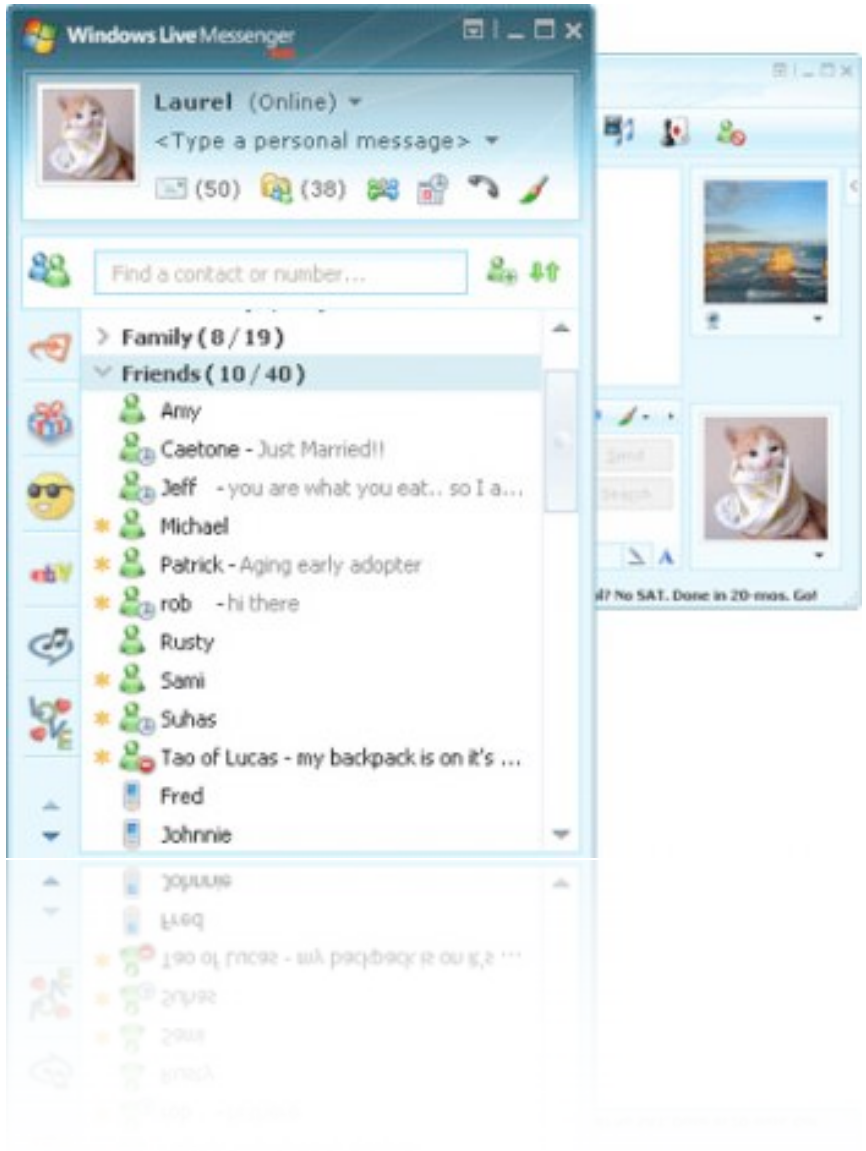


Salt derivation algorithm overview



Microsoft Messenger

- Encryption
  DPAPI or Credstore
- Difficulty
  Medium
- Location
  version dependent



Amy
Caetone - Just Married!!
Jeff - you are what you eat.. so I a...
Michael
Patrick - Aging early adopter
rob - hi there
Rusty
Sami
Suhas
Tao of Lucas - my backpack is on it's ...
Fred
Johnnie

Windows Messenger by version

Version	Storage	encryption
5	Registry	Base64 encoded
6	Credstore	Credstore
7	Registry x2	DPAPI x 2
Live	Credstore	Credstore

aMSN

- Encryption

  DES

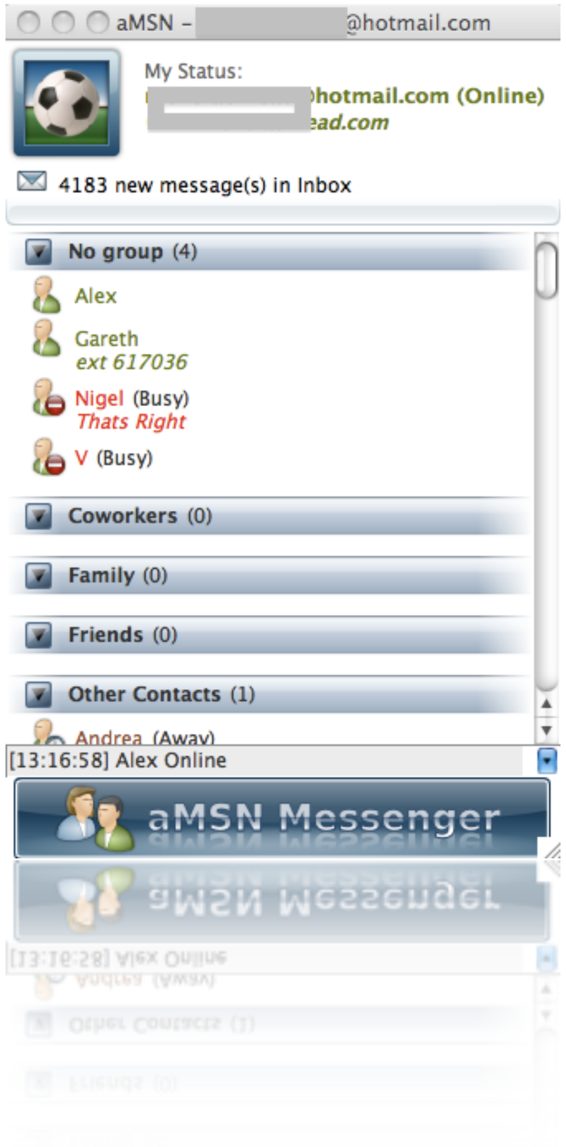
  key: substr(login . “dummykey”, 8)

- Difficulty

  easy

- Location

  config.xml



aMSN – [redacted]@hotmail.com

My Status:

[redacted]hotmail.com (Online)

[redacted]ead.com

4183 new message(s) in Inbox

[13:16:58] Alex Online

9talk

- Encryption
  XOR
  key: 9
- Difficulty
  trivial
- Location
  user.config

Afin de ne perdre aucun message, vos appels en absence ou lorsque vous n'etes pas connectés sont redirigés vers votre boite vocale.

Vous pouvez écouter vos messages en appelant le *9 depuis votre domicile ou depuis le site http://voicemail.neuf.fr/

Trillian

- Encryption

  Base 64 +XOR

  key: fixed string

- Difficulty

  trivial

- Location

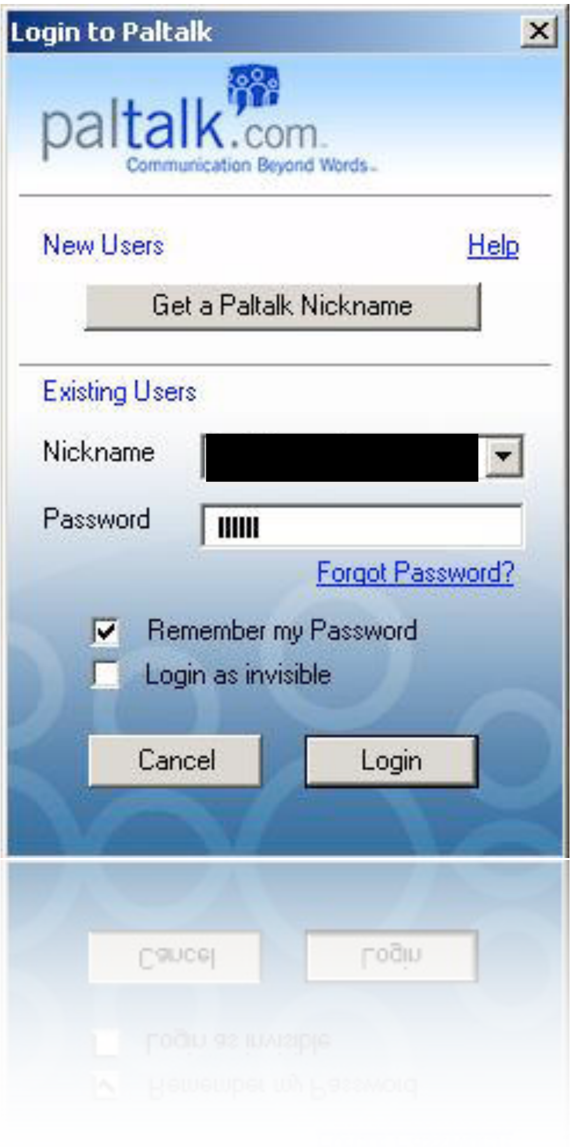
  user.config

Pidgin

- Encryption
  Clear aka encryt-what?
- Difficulty
  none
- Location
  account.xml

Paltalk

- Encryption
  Custom
- Difficulty
  difficult (offline)
- Location
  registry



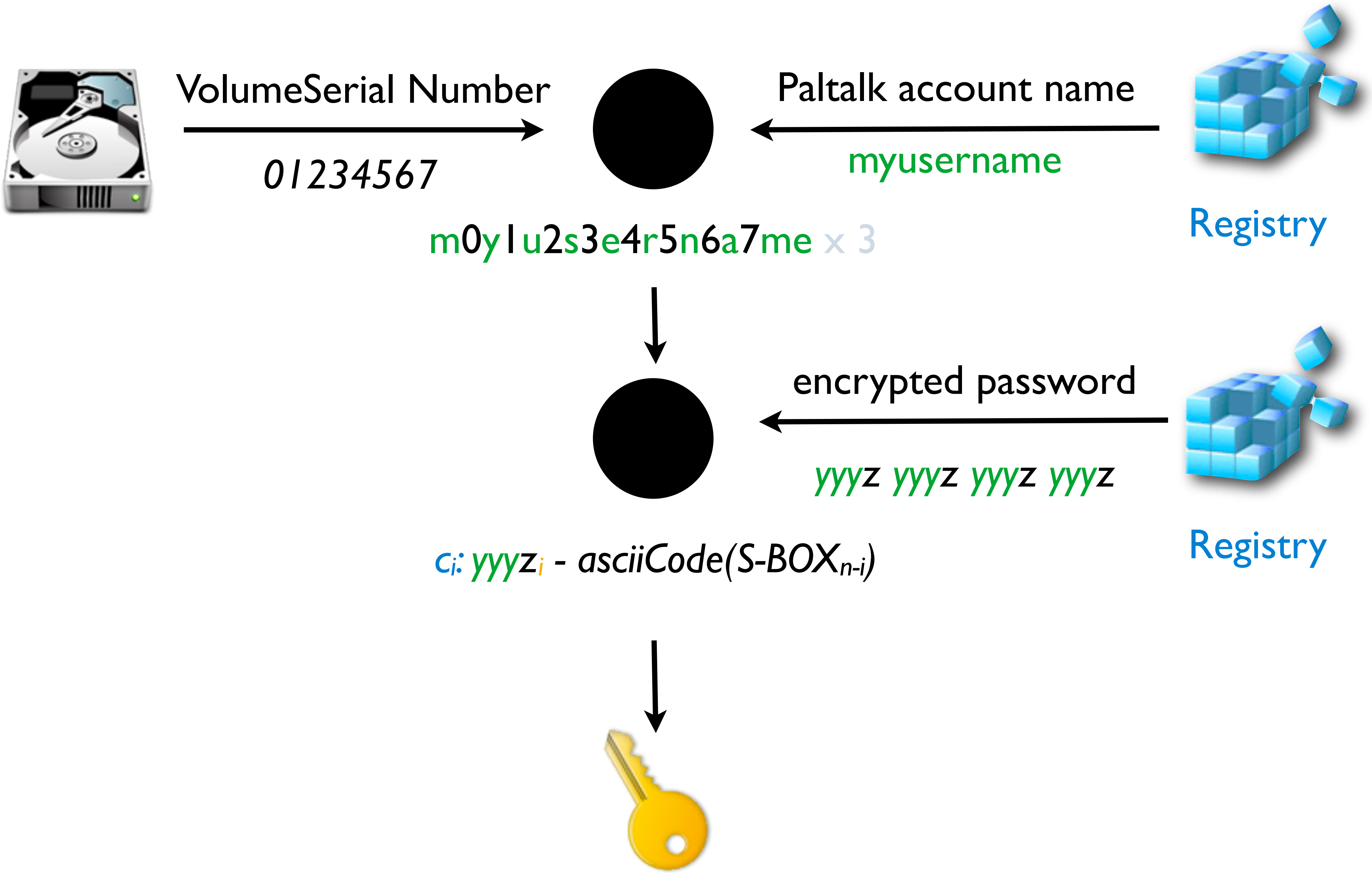
Nickname [redacted]

Password IIIIII

☑ Remember my Password

□ Login as invisible

Paltalk encryption algorithm



VolumeSerial Number

01234567

Paltalk account name

myusername

Registry

m0y1u2s3e4r5n6a7me x 3

encrypted password

yyyz yyyz yyyz yyyz

Registry

c_i: *$yyyz_i$ - asciiCode(S-BOX$_{n-i}$)*

Messenger take away

- If the Skype password is strong you can’t recover it
- Gtalk and Paltalk are the only ones to use computer information
- 3rd party software are the least secure

Conclusion

- People moving to the cloud means more data that is harder to get
- Forensics needs to evolve to cope with this
- OWADE is the first tool dedicated to cloud forensic
  - Decrypt the 4 major browsers data
  - Decrypt Instant messaging credentials
  - Open-source

Download OWADE

http://owade.org

Follow-us on Twitter

@elie, @owade

Donate to OWADE to support it !