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

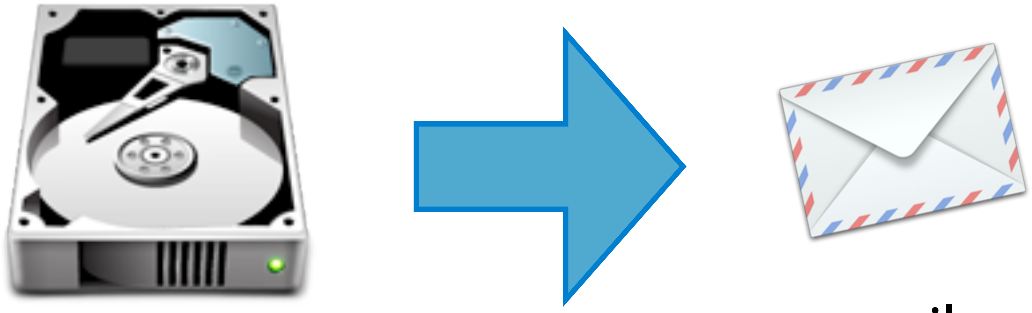
2.7 millions photos are uploaded to Facebook every 20 minutes

100 millions new files are saved on Dropbox every day

Data are moving to multiple services

Hard drive

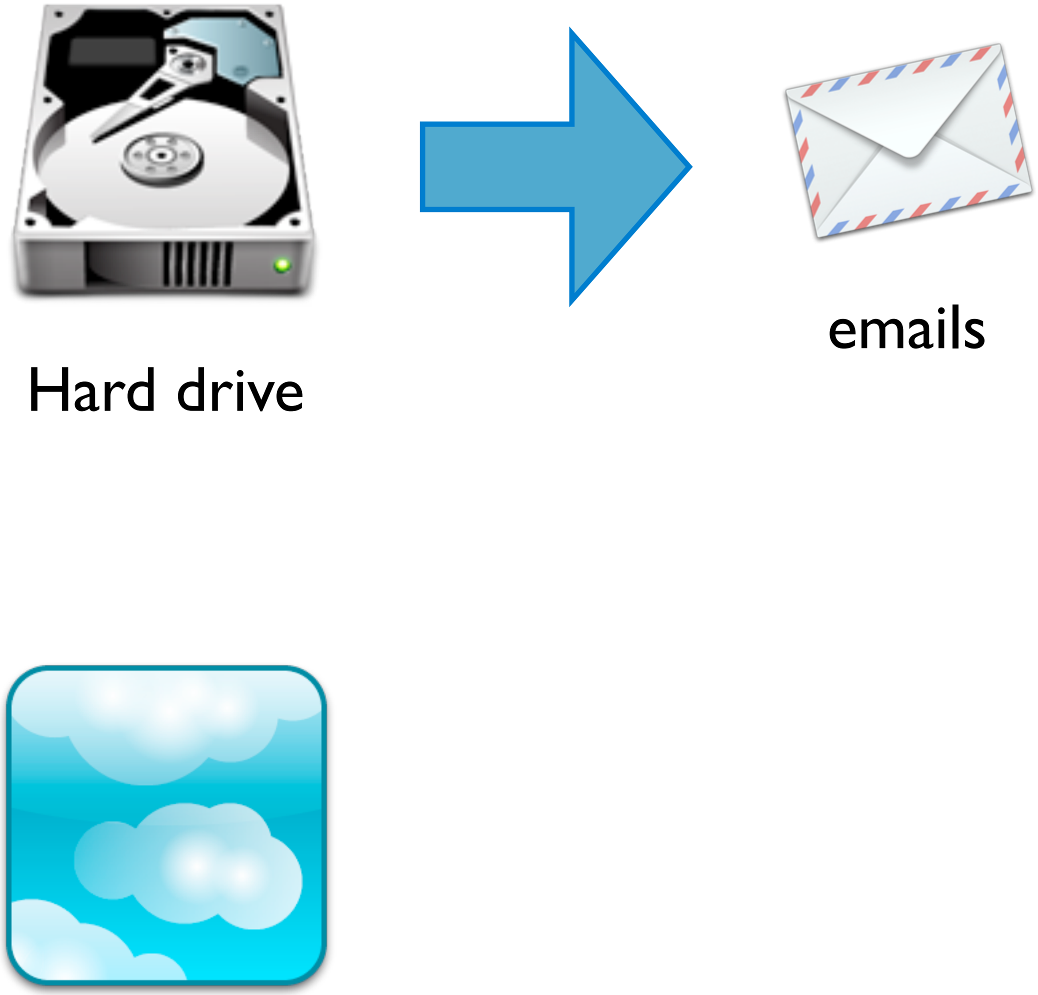
Data are moving to multiple services



Hard drive

emails

Data are moving to multiple services

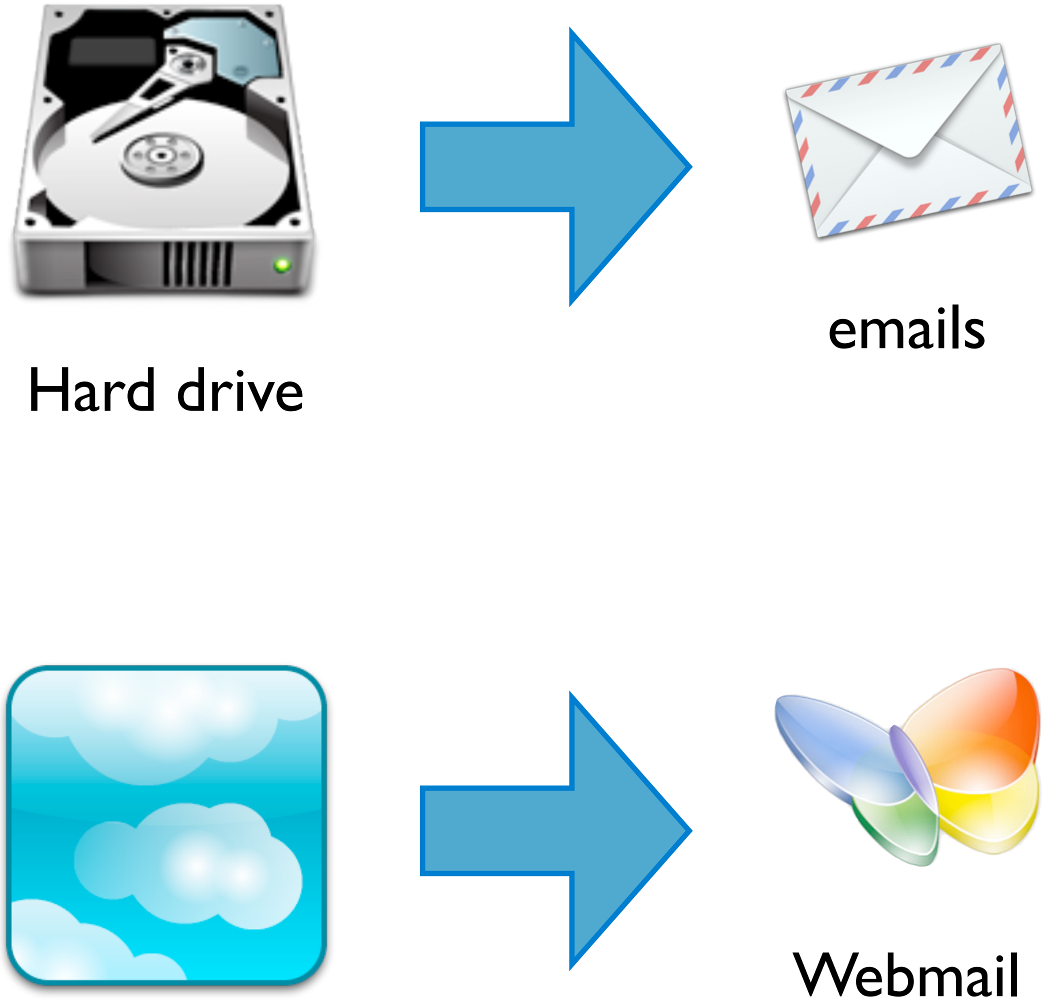


Hard drive

emails

Cloud

Data are moving to multiple services



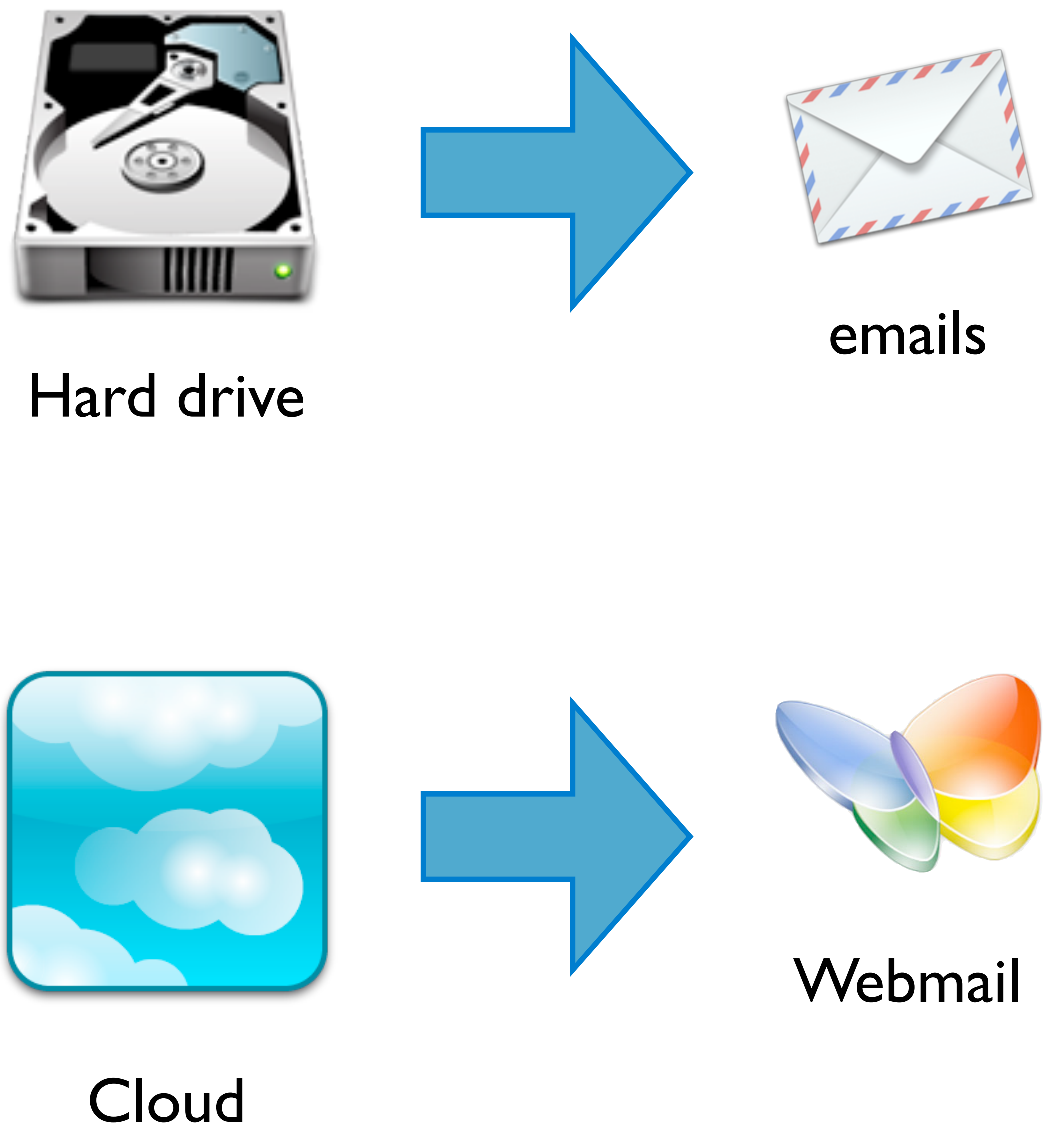
Hard drive

emails

Cloud

Webmail

Data are moving to multiple services



Hard drive

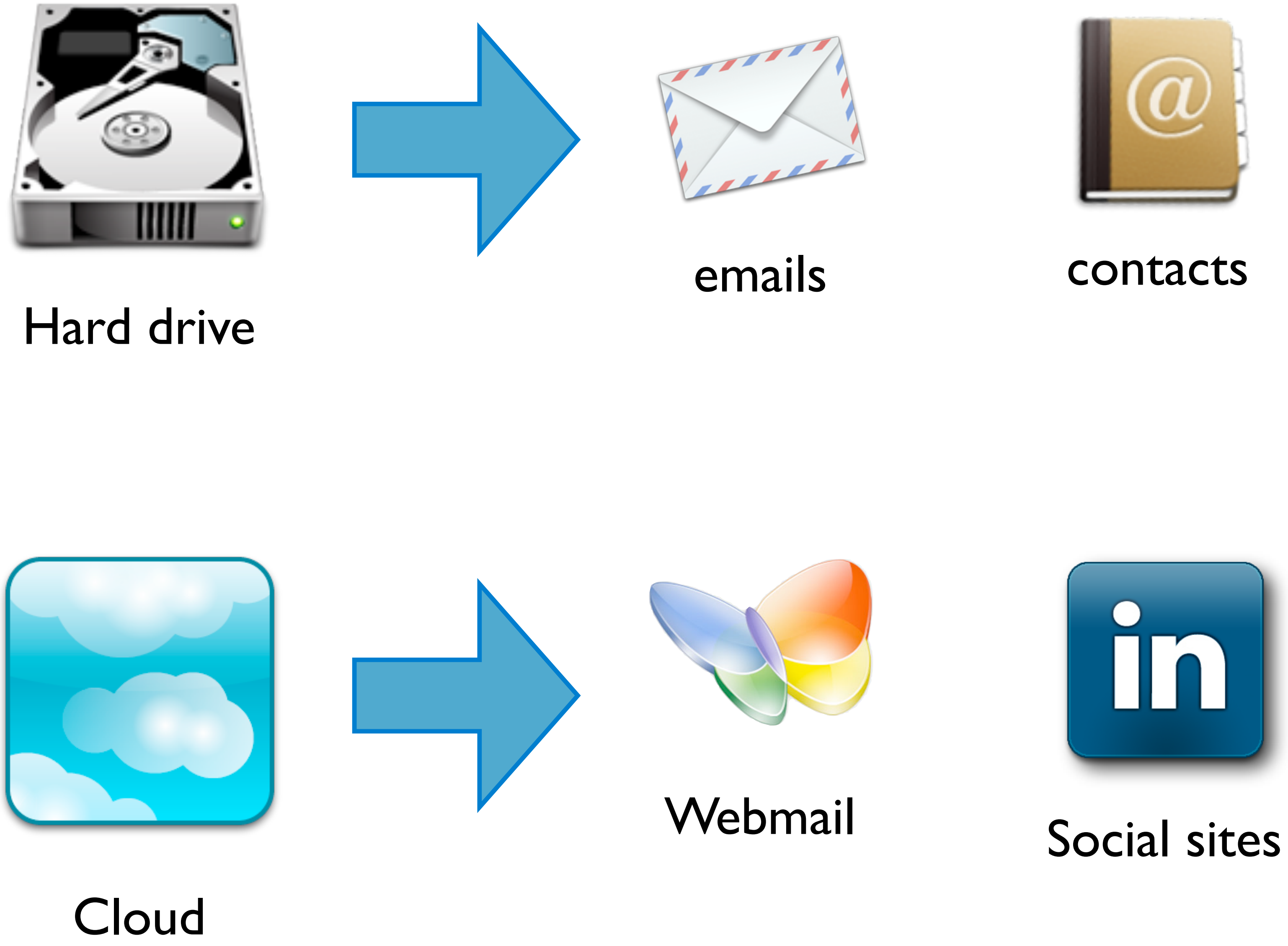
emails

contacts

Cloud

Webmail

Data are moving to multiple services



Hard drive

emails

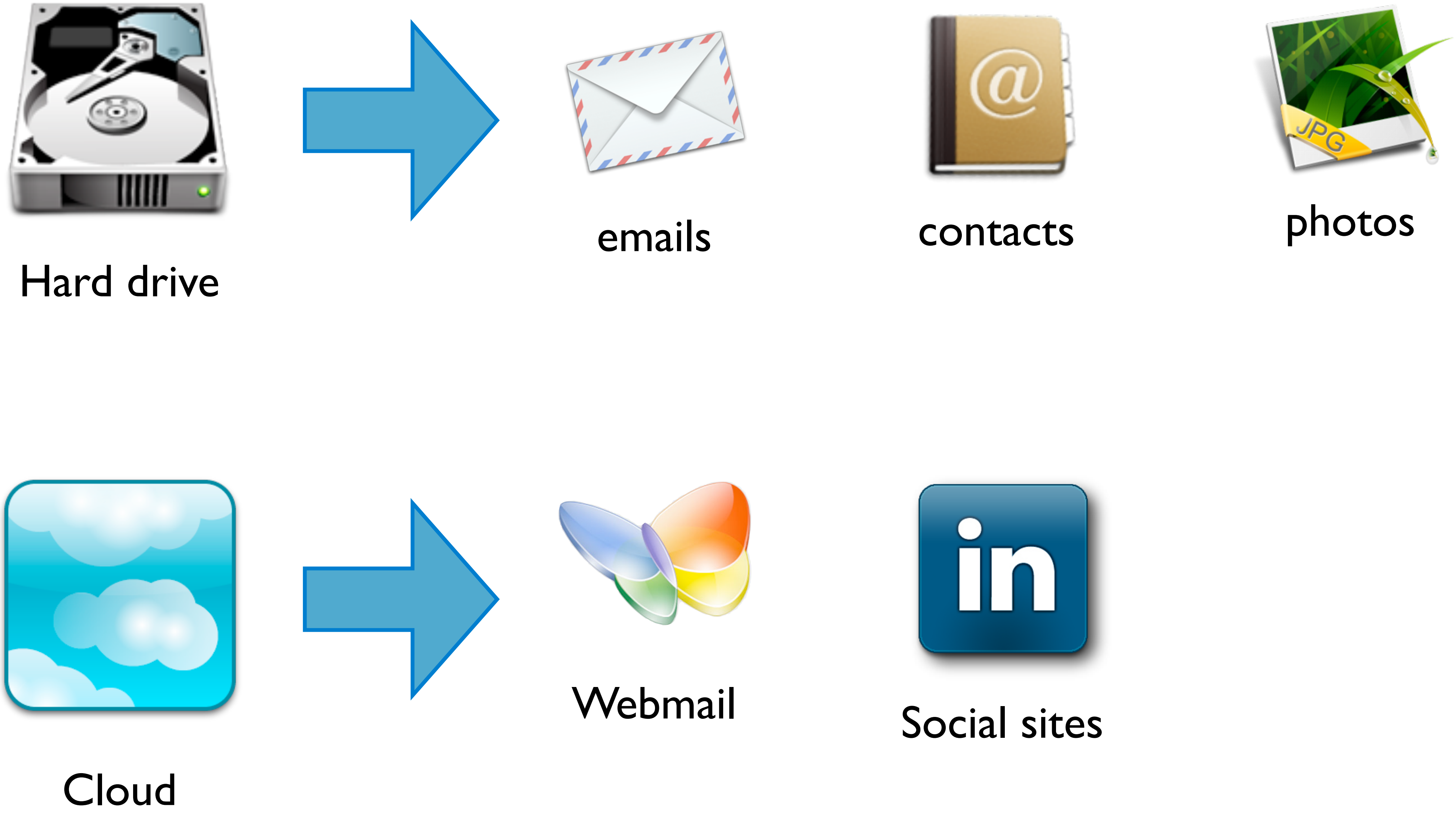
contacts

Cloud

Webmail

Social sites

Data are moving to multiple services



Hard drive

emails

contacts

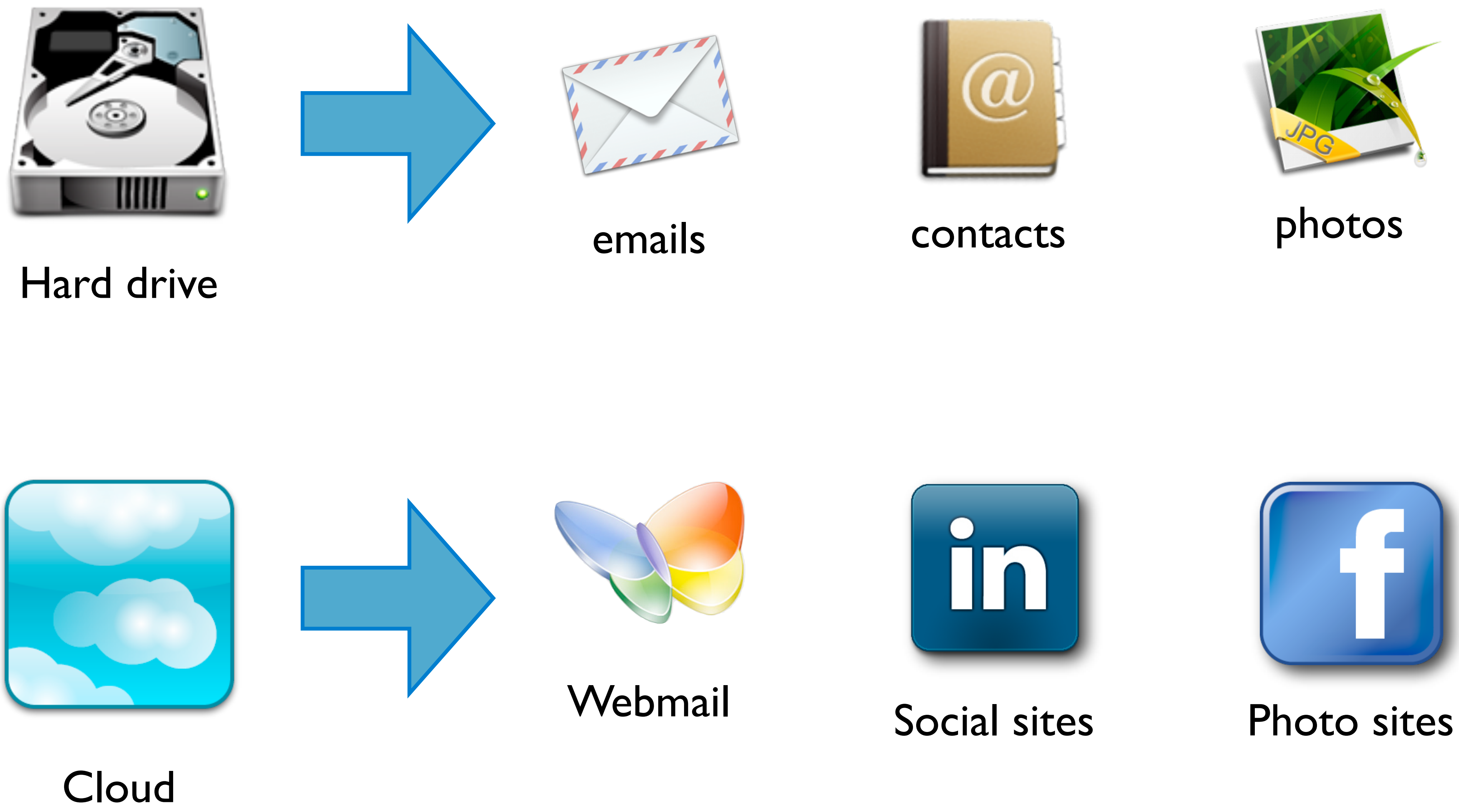
photos

Cloud

Webmail

Social sites

Data are moving to multiple services



Hard drive

emails

contacts

photos

Cloud

Webmail

Social sites

Photo sites

Impact on the forensic field

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

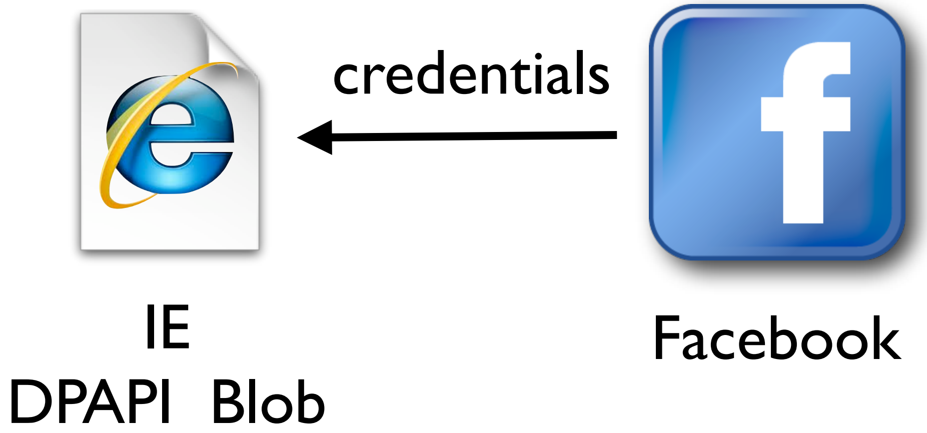
Let’s do cloud forensics

What is cloud forensics ?

Facebook credentials as a use case

Facebook

Facebook credentials as a use case

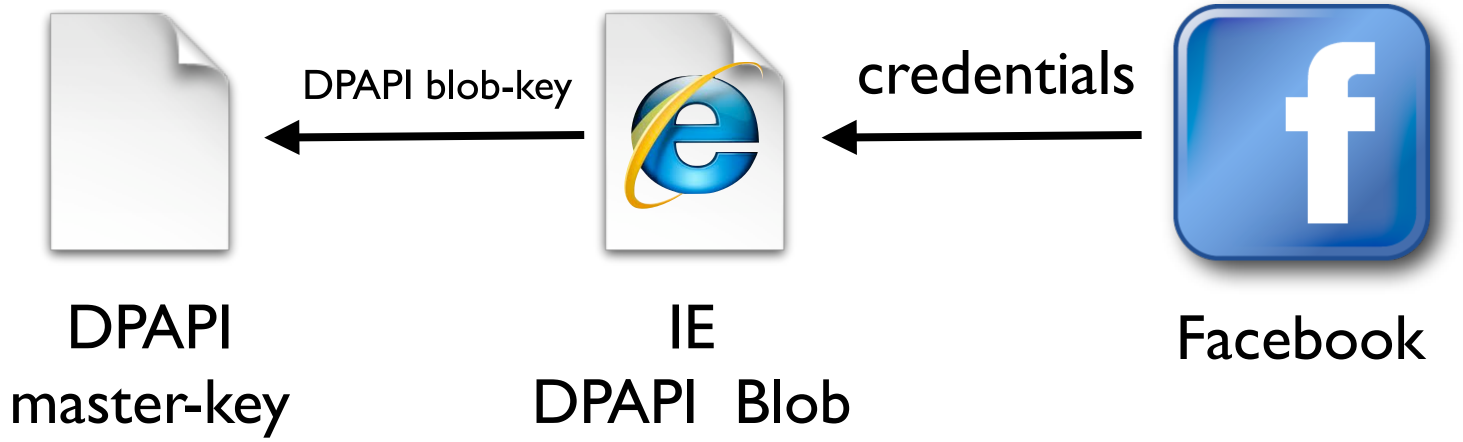


credentials

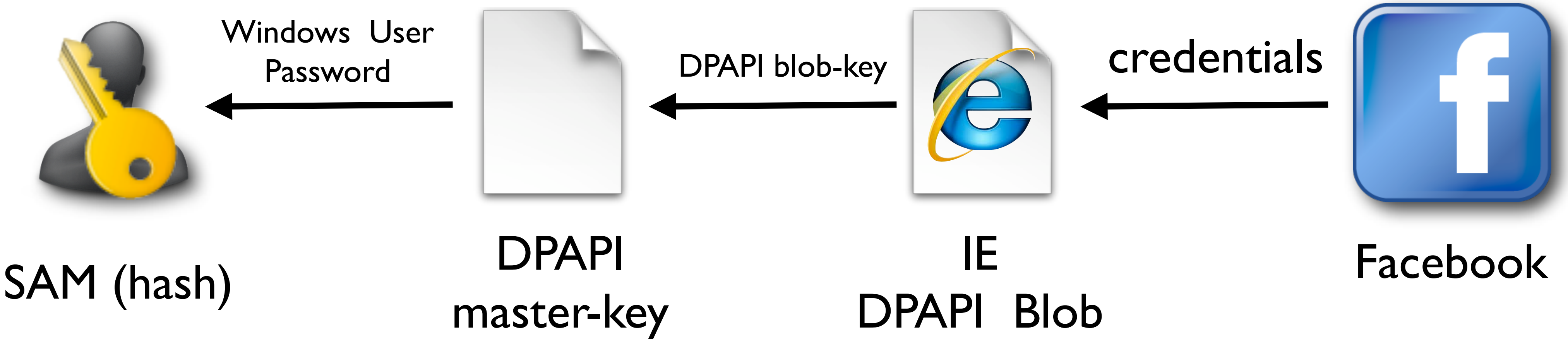
IE
DPAPI Blob

Facebook

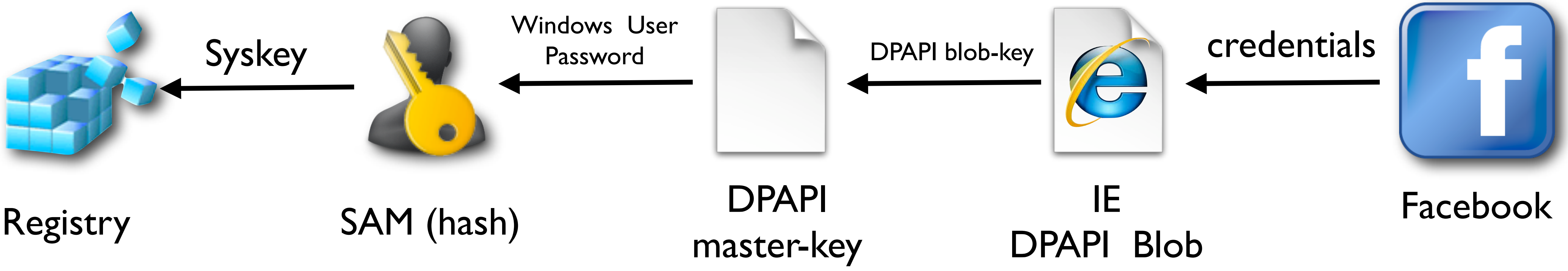
Facebook credentials as a use case



Facebook credentials as a use case

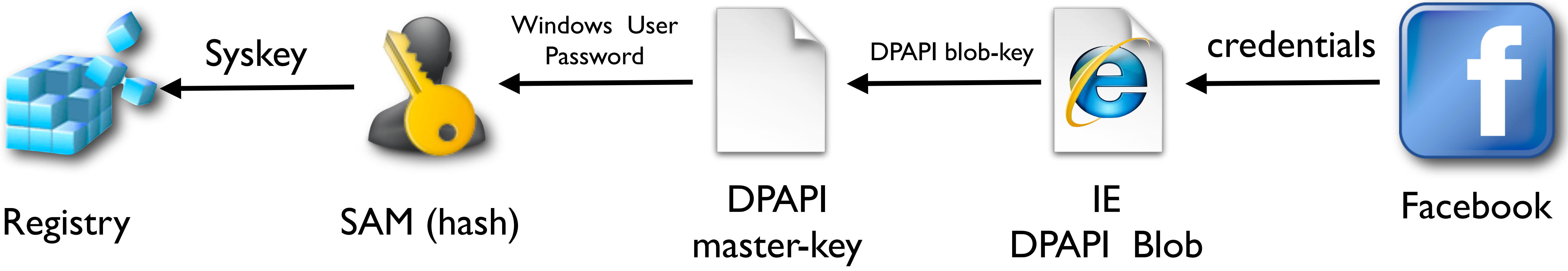


Facebook credentials as a use case



Registry ← Syskey ← SAM (hash) ← Windows User Password ← DPAPI master-key ← DPAPI blob-key ← IE DPAPI Blob ← credentials ← Facebook

Facebook credentials as a use case



Registry

Syskey

SAM (hash)

Windows User Password

DPAPI master-key

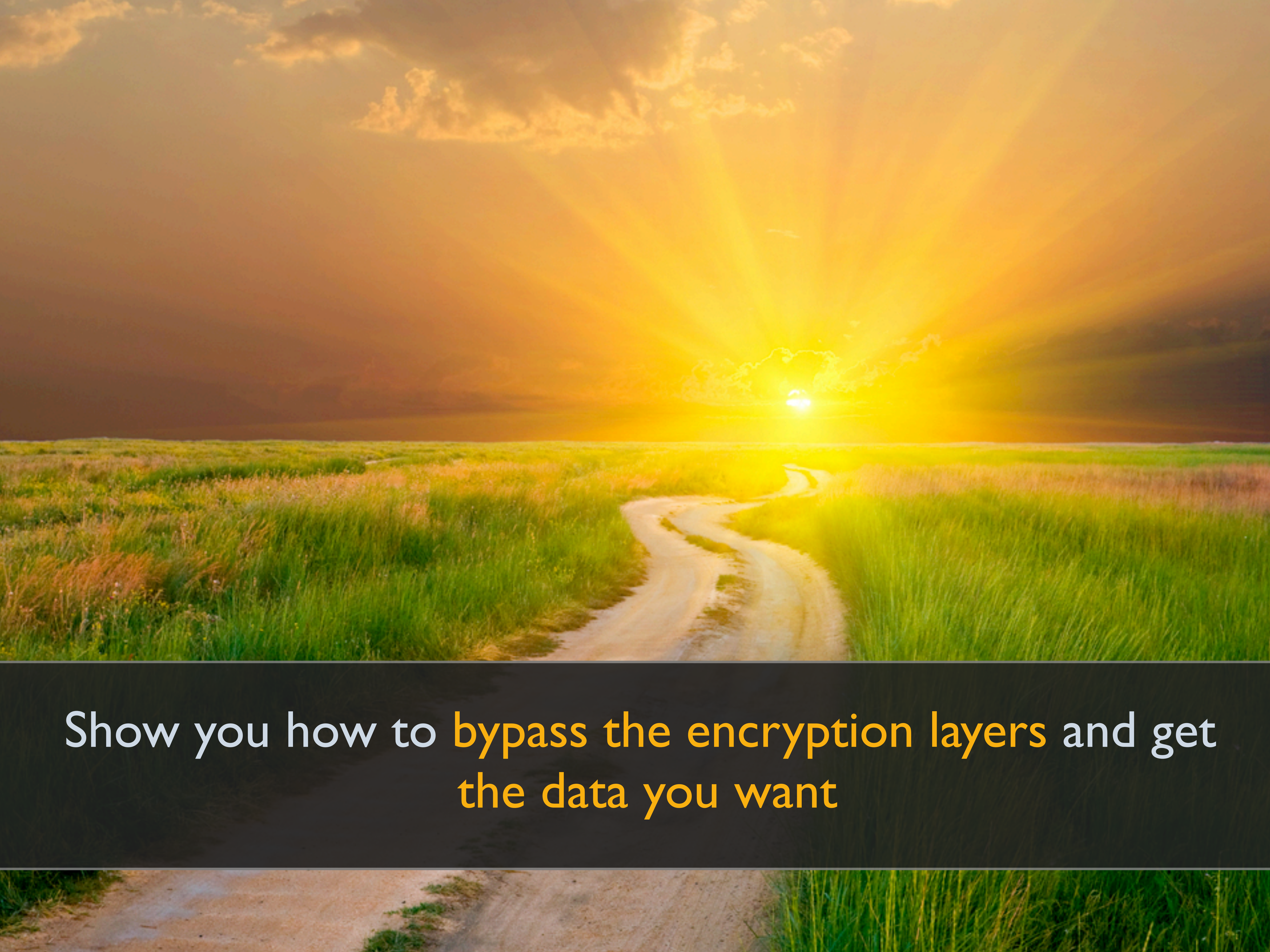
DPAPI blob-key

IE DPAPI Blob

credentials

Facebook

Getting Facebook credentials require to bypass 4 layers of encryption



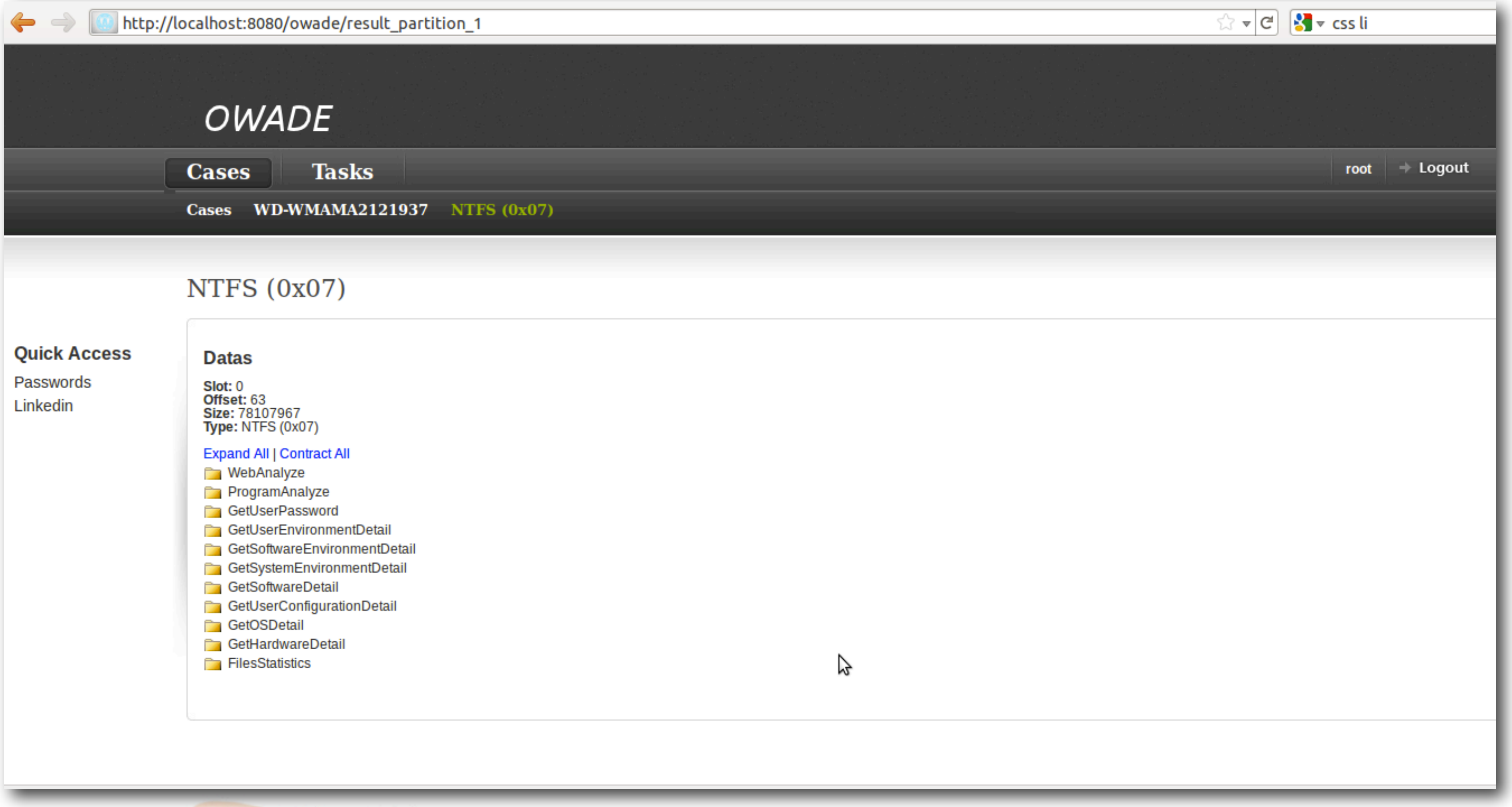
Show you how to bypass the encryption layers and get the data you want

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 in action



NTFS (0x07)

Datas

Slot: 0
Offset: 63
Size: 78107967
Type: NTFS (0x07)

- WebAnalyze
- ProgramAnalyze
- GetUserPassword
- GetUserEnvironmentDetail
- GetSoftwareEnvironmentDetail
- GetSystemEnvironmentDetail
- GetSoftwareDetail
- GetUserConfigurationDetail
- GetOSDetail
- GetHardwareDetail
- FilesStatistics

OWADE overview

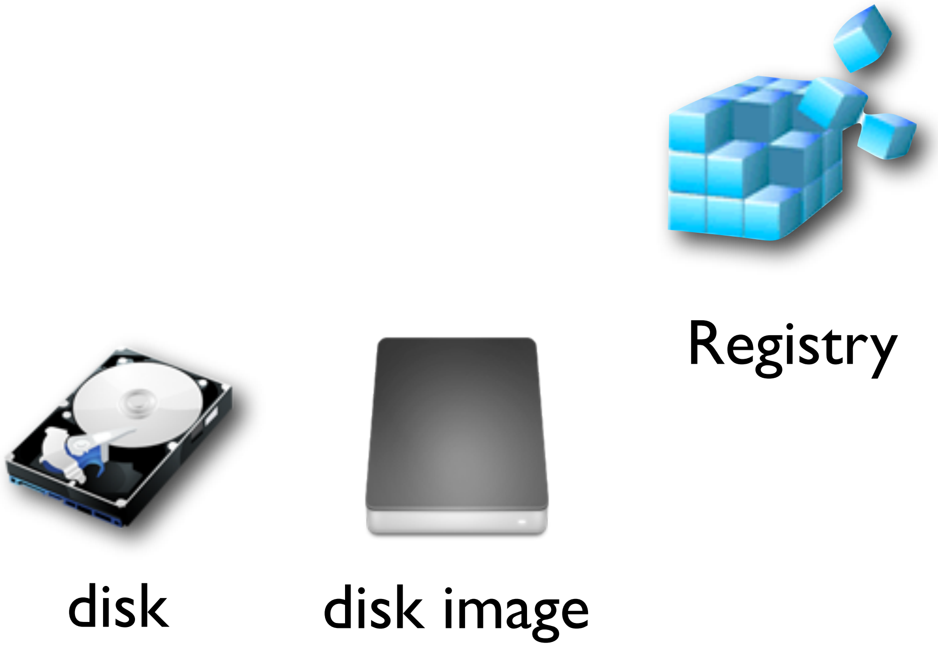
OWADE overview

OWADE overview

disk

disk image

OWADE overview



Registry

disk

disk image

OWADE overview

disk

disk image

Registry

Files

OWADE overview

Windows credentials

Registry

disk

disk image

Files

OWADE overview

Windows credentials

Registry

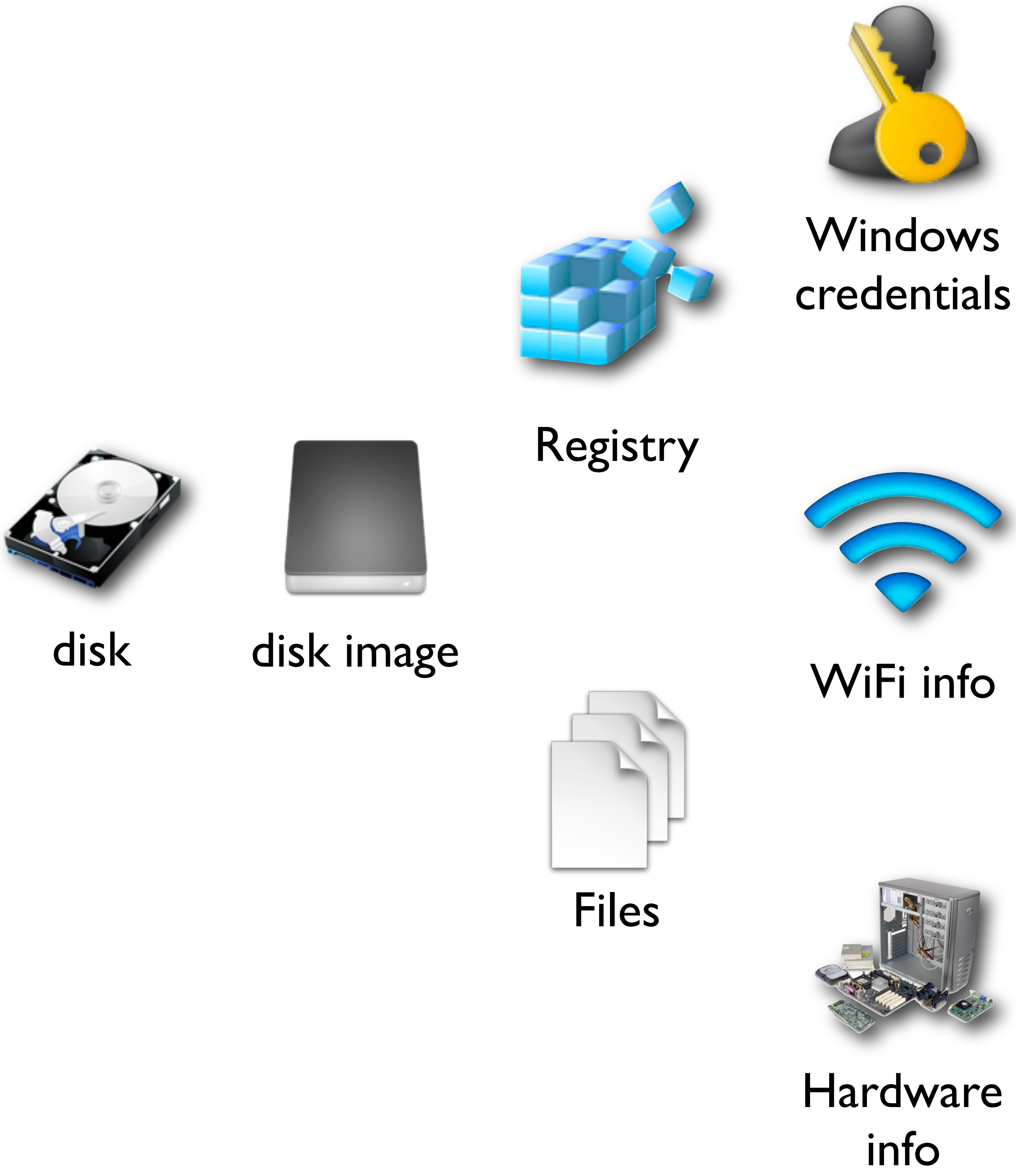
disk

disk image

WiFi info

Files

OWADE overview



disk

disk image

Registry

Files

Windows credentials

WiFi info

Hardware info

OWADE overview

disk

disk image

Registry

Files

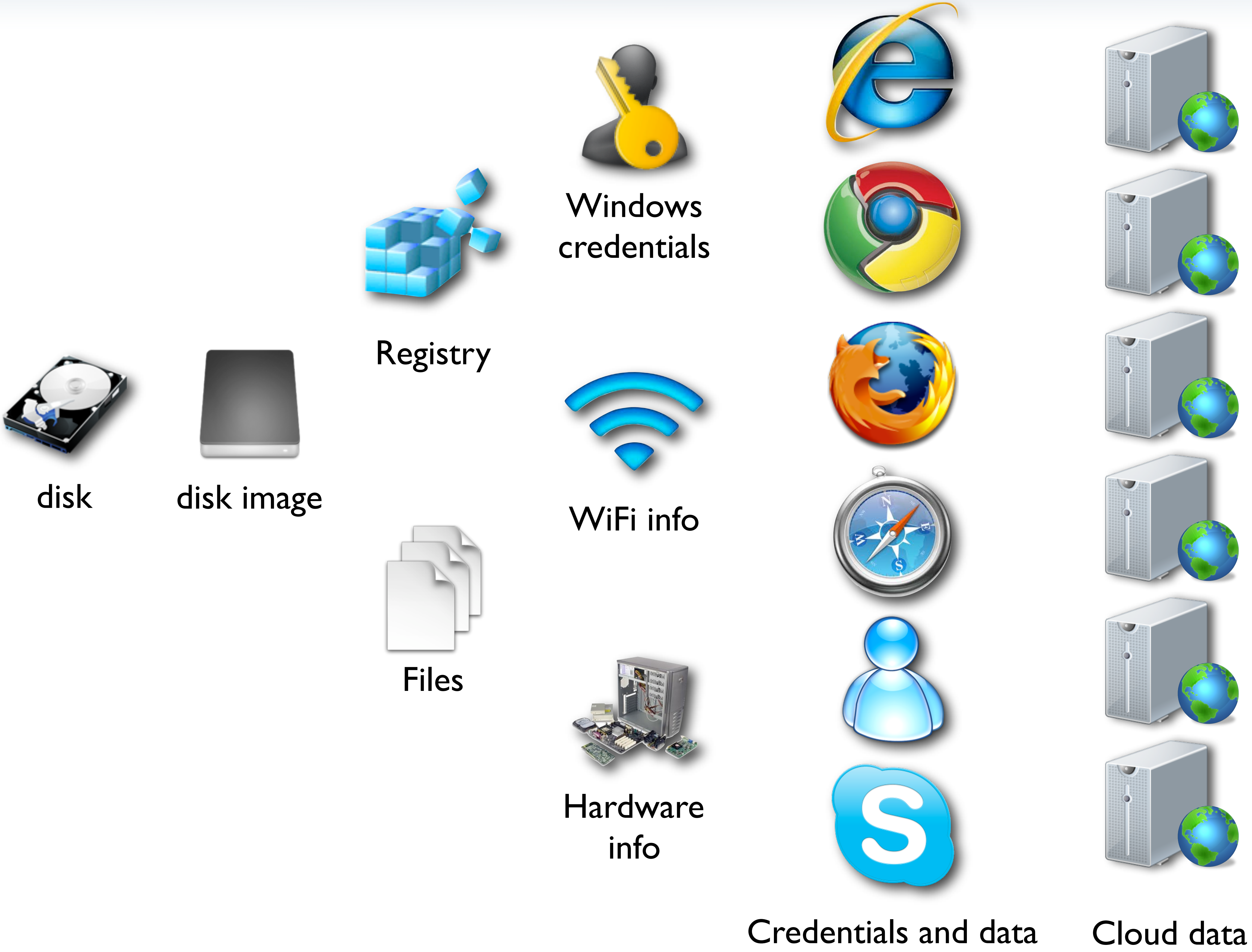
Windows credentials

WiFi info

Hardware info

Credentials and data

OWADE overview



disk

disk image

Registry

Files

Windows credentials

WiFi info

Hardware info

Credentials and data

Cloud data

Outline

Outline

- File base forensics refresher

Outline

- File base forensics refresher
- The Windows crypto eco-system

Outline

- File base forensics refresher
- The Windows crypto eco-system
- Wifi data and Geo-location

Outline

- File base forensics refresher
- The Windows crypto eco-system
- Wifi data and Geo-location
- Recovering browser data

Outline

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

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

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

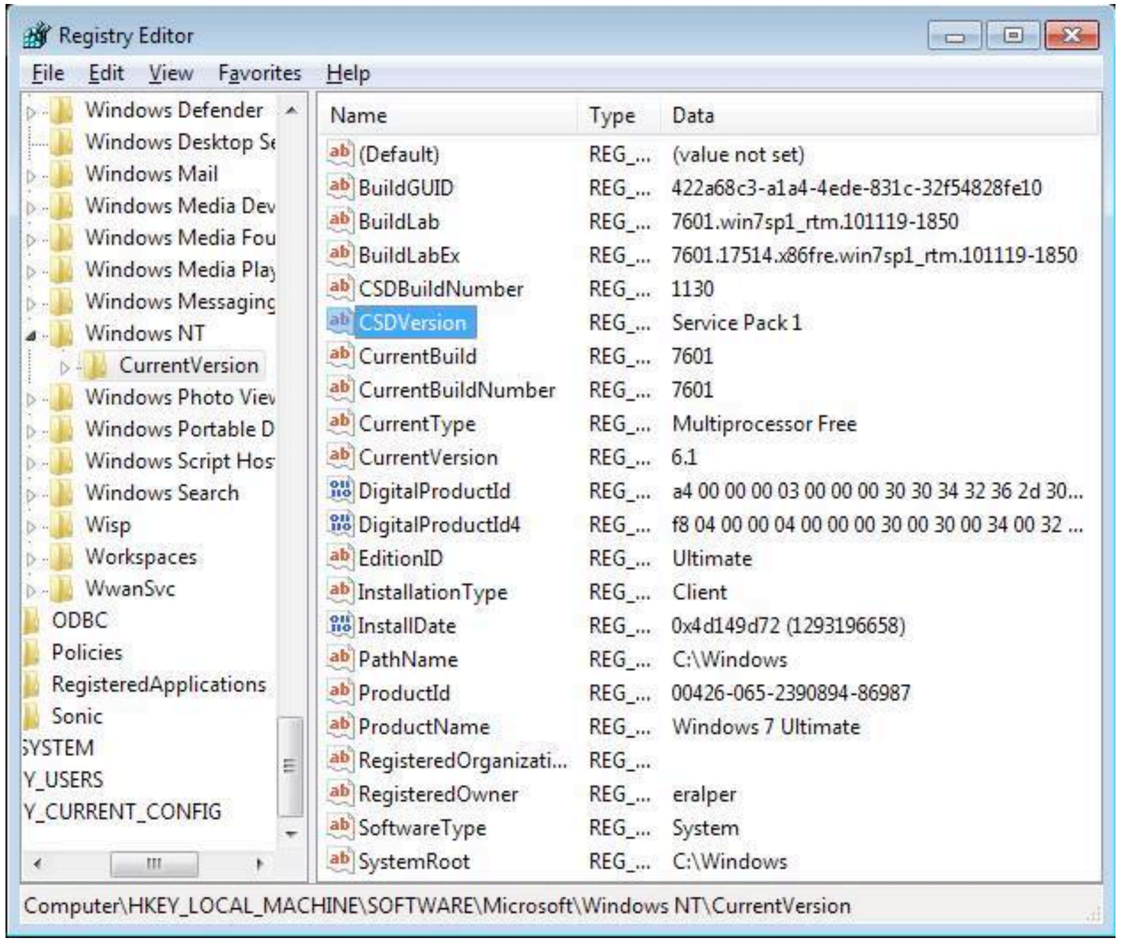
File based forensic refresher

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

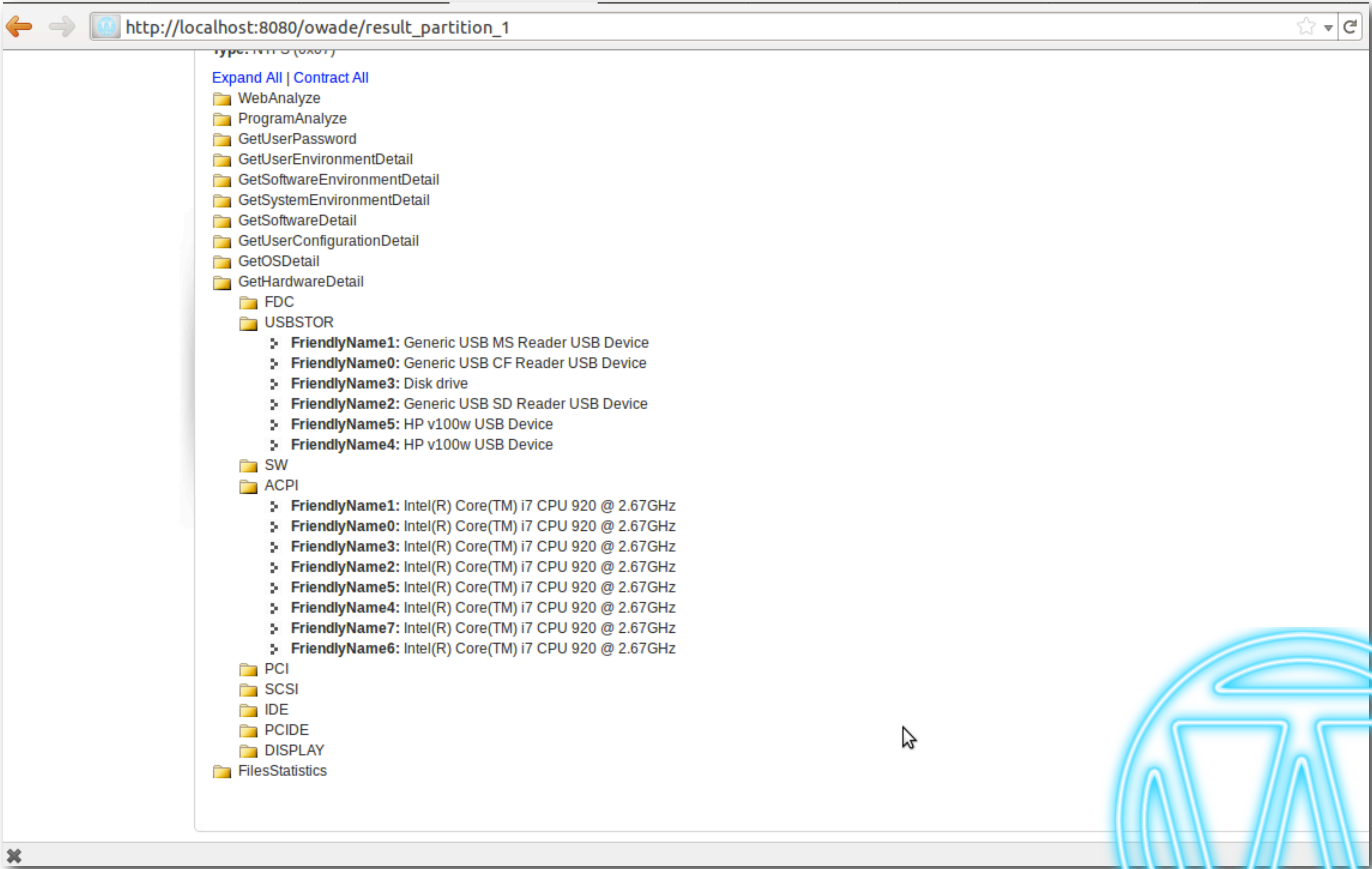
- .dat files
- Hardware information
- Softwares installed with their versions and serials
- Windows credentials (encrypted)



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

Some Registry Information Extracted



http://localhost:8080/owade/result_partition_1

Type: NTFS (0x07)

Expand All | Contract All

- WebAnalyze
- ProgramAnalyze
- GetUserPassword
- GetUserEnvironmentDetail
- GetSoftwareEnvironmentDetail
- GetSystemEnvironmentDetail
- GetSoftwareDetail
- GetUserConfigurationDetail
- GetOSDetail
- GetHardwareDetail
  - FDC
  - USBSTOR
    - **FriendlyName1:** Generic USB MS Reader USB Device
    - **FriendlyName0:** Generic USB CF Reader USB Device
    - **FriendlyName3:** Disk drive
    - **FriendlyName2:** Generic USB SD Reader USB Device
    - **FriendlyName5:** HP v100w USB Device
    - **FriendlyName4:** HP v100w USB Device
  - SW
  - ACPI
    - **FriendlyName1:** Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
    - **FriendlyName0:** Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
    - **FriendlyName3:** Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
    - **FriendlyName2:** Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
    - **FriendlyName5:** Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
    - **FriendlyName4:** Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
    - **FriendlyName7:** Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
    - **FriendlyName6:** Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
  - PCI
  - SCSI
  - IDE
  - PCIDE
  - DISPLAY
- FilesStatistics

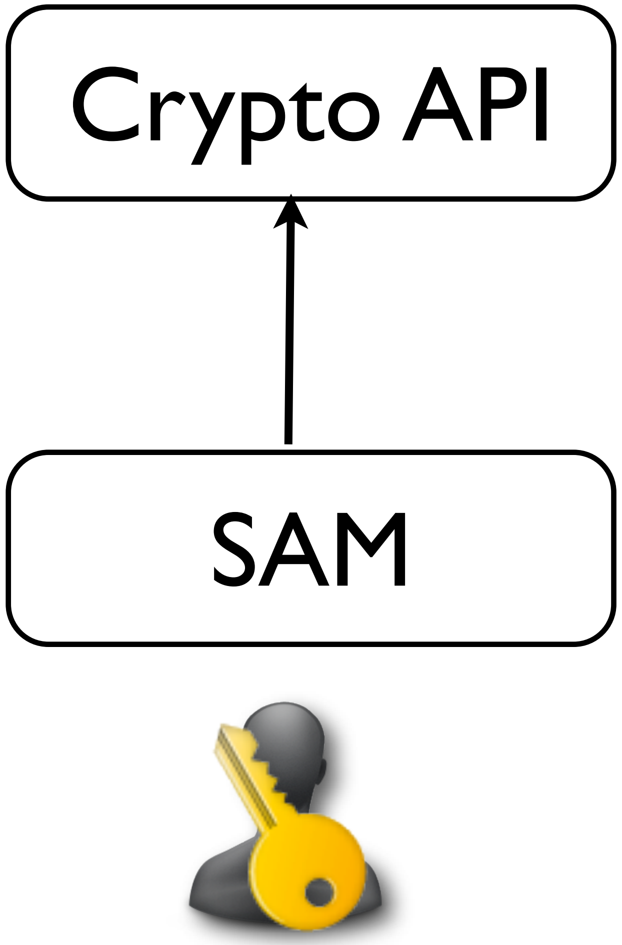
Windows crypto

Why do we care about Windows crypto ?

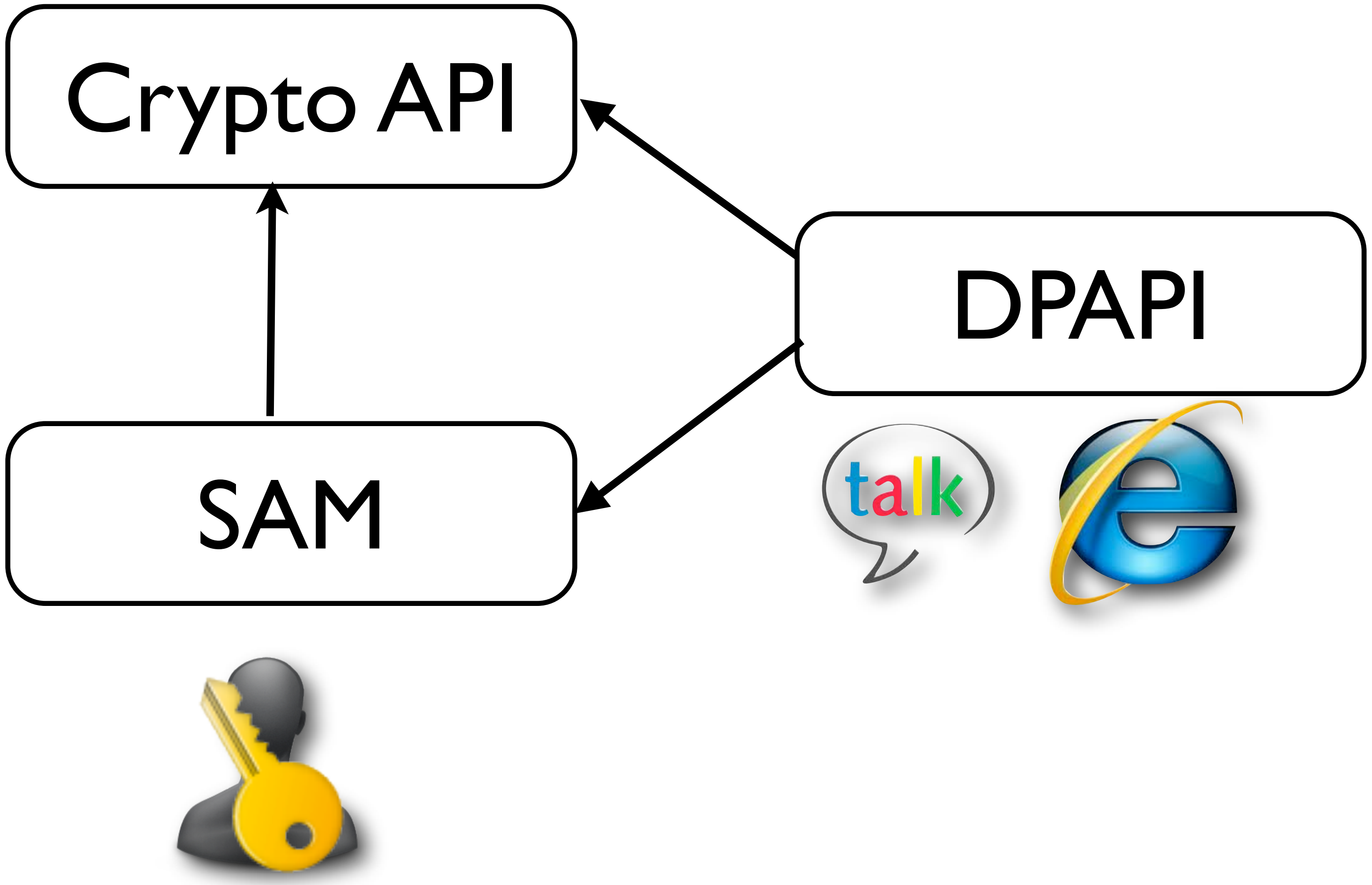
The Windows crypto eco-system

Crypto API

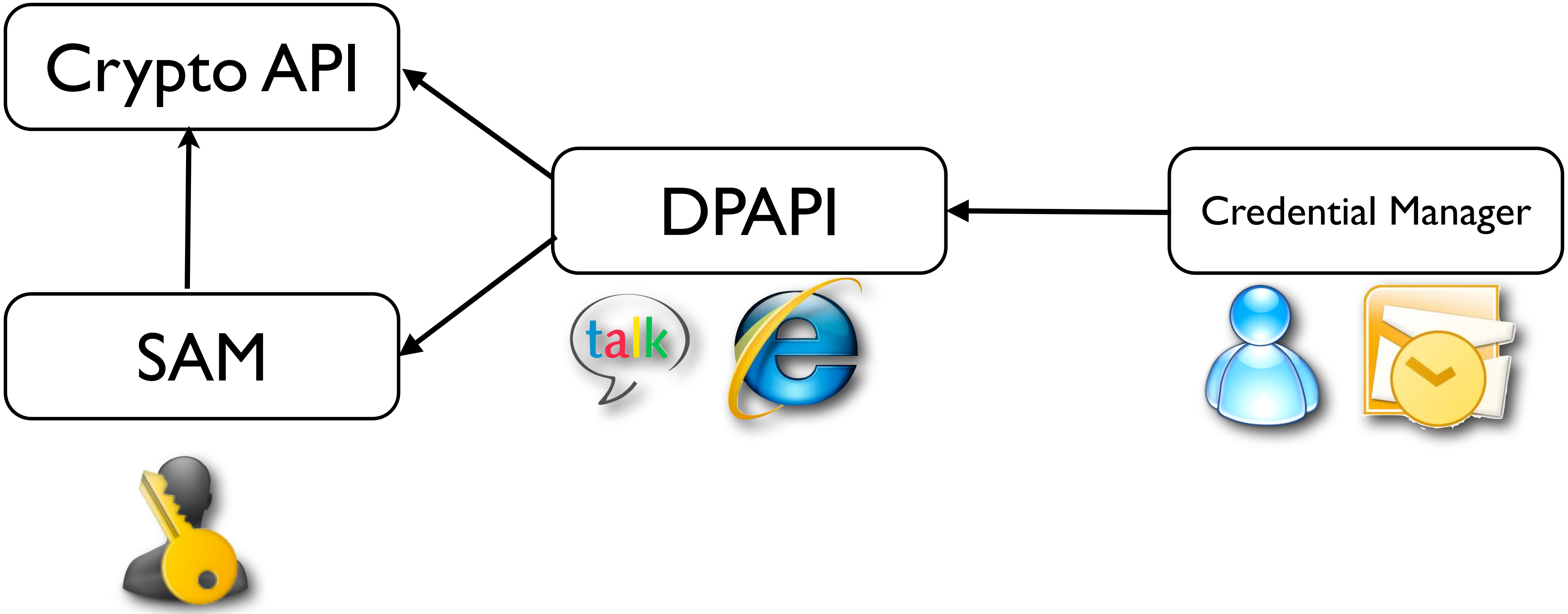
The Windows crypto eco-system



The Windows crypto eco-system



The Windows crypto eco-system

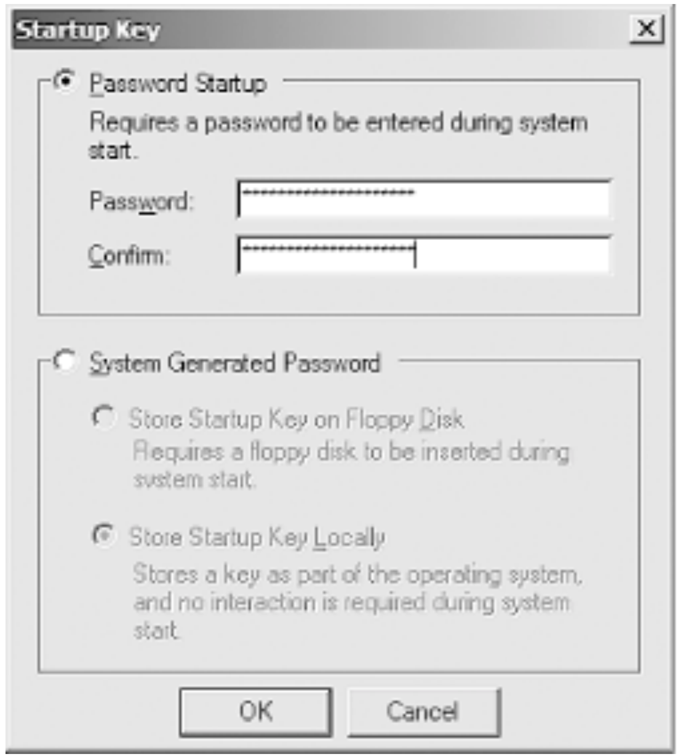


Windows Crypto API

- 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
- Passwords 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)
- Passwords 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)

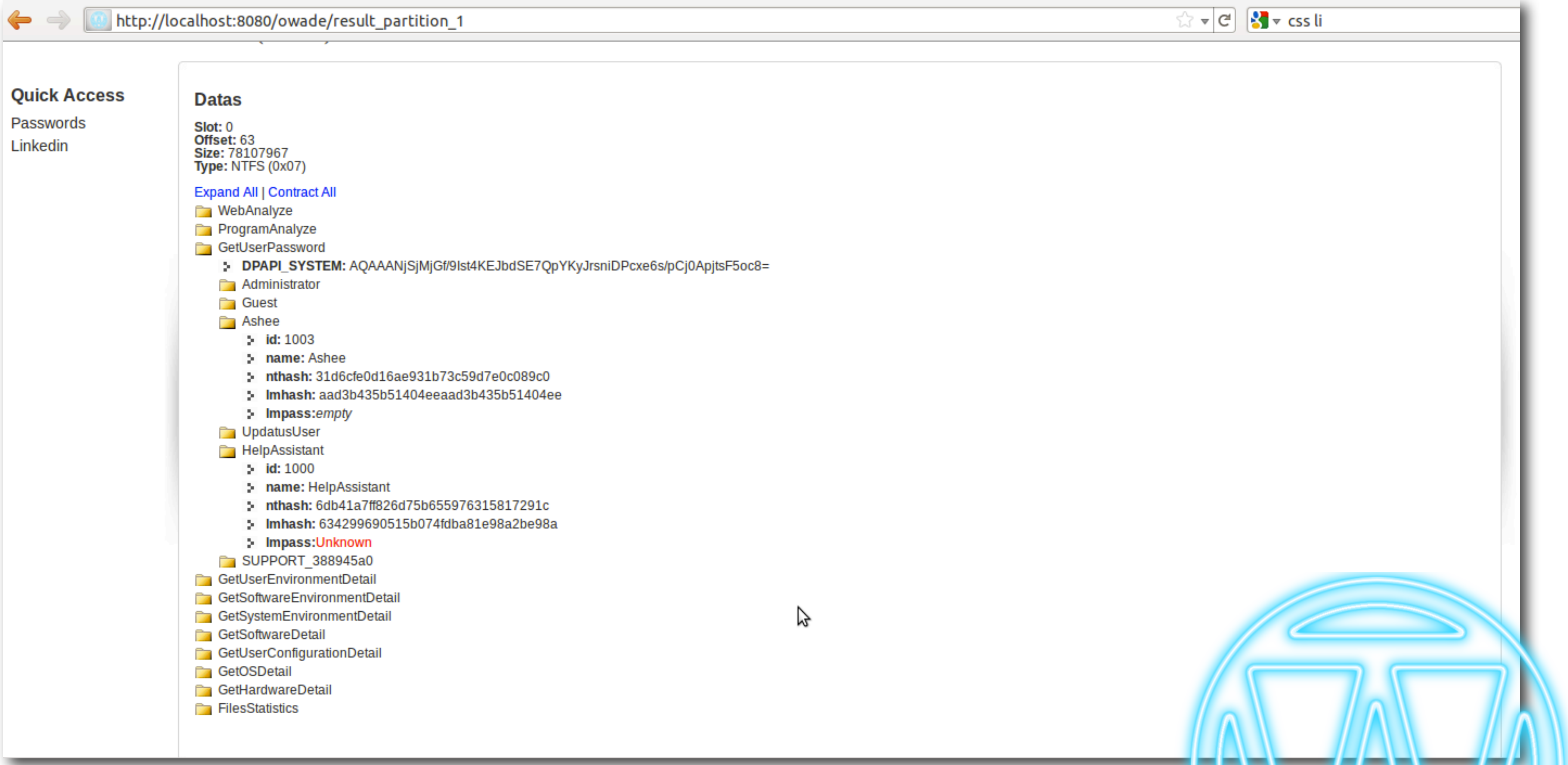
Rainbow Tables

- 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

Windows Password recovered


http://localhost:8080/owade/result_partition_1

Quick Access

Passwords

Linkedin

Datas

Slot: 0
Offset: 63
Size: 78107967
Type: NTFS (0x07)

Expand All | Contract All

```
WebAnalyze
ProgramAnalyze
GetUserPassword
    DPAPI_SYSTEM: AQAAANjSjMjGf/9Ist4KEJbdSE7QpYKyJrsniDPcxe6s/pCj0ApjtsF5oc8=
    Administrator
    Guest
    Ashee
        id: 1003
        name: Ashee
        nthash: 31d6cfe0d16ae931b73c59d7e0c089c0
        lmhash: aad3b435b51404eeaad3b435b51404ee
        lmpass:empty
    UpdatusUser
    HelpAssistant
        id: 1000
        name: HelpAssistant
        nthash: 6db41a7ff826d75b655976315817291c
        lmhash: 634299690515b074fdba81e98a2be98a
        lmpass:Unknown
    SUPPORT_388945a0
GetUserEnvironmentDetail
GetSoftwareEnvironmentDetail
GetSystemEnvironmentDetail
GetSoftwareDetail
GetUserConfigurationDetail
GetOSDetail
GetHardwareDetail
FilesStatistics
```

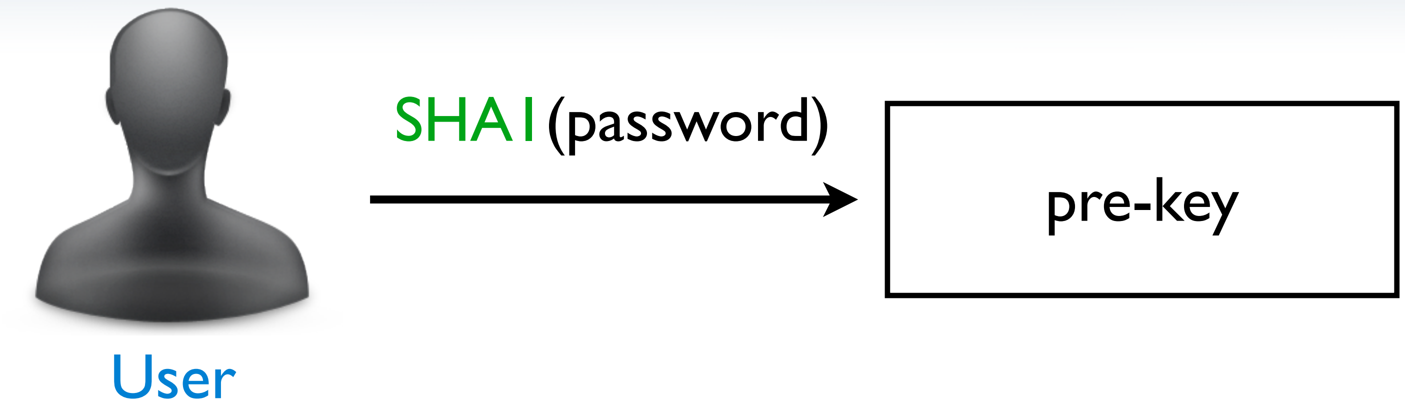
If the password is too strong we can’t recover it

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
- Main point : tie the encryption to the user password

DPAPI derivation scheme

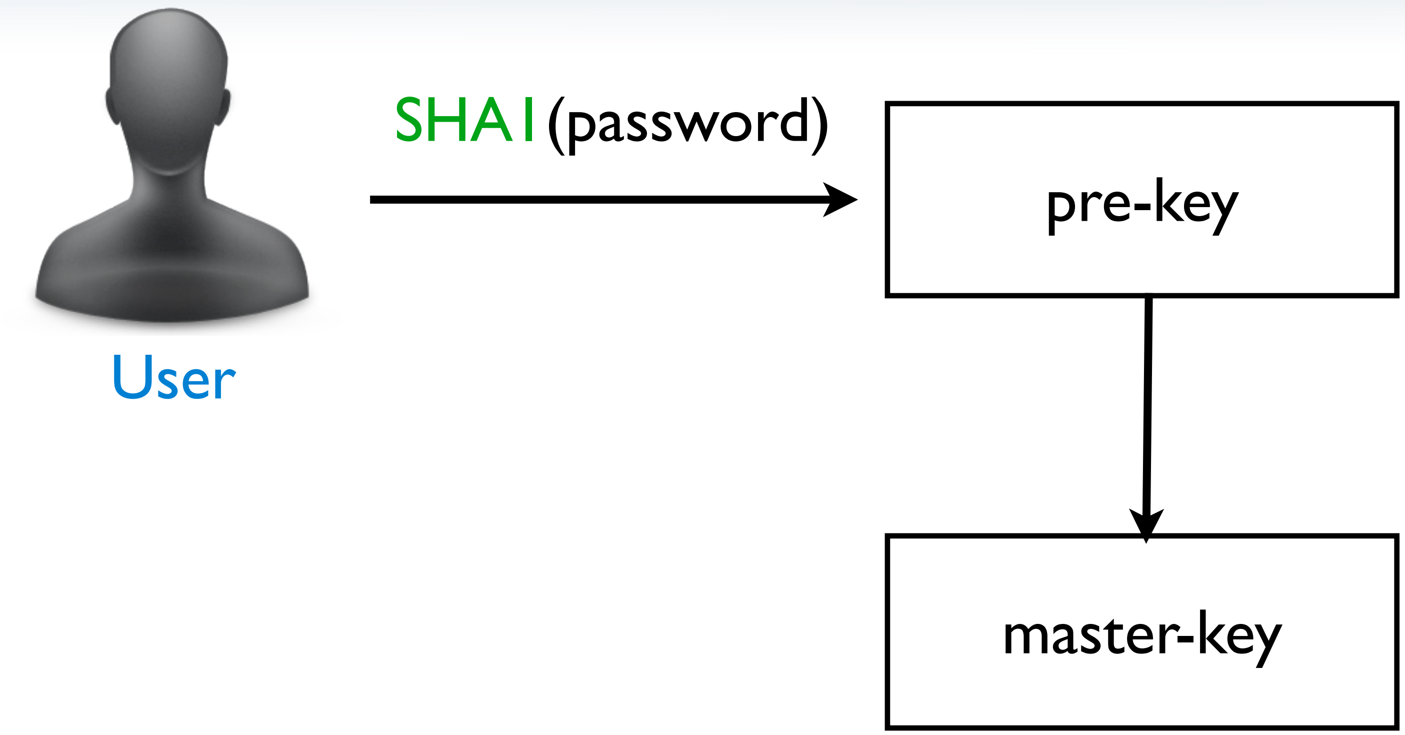


User

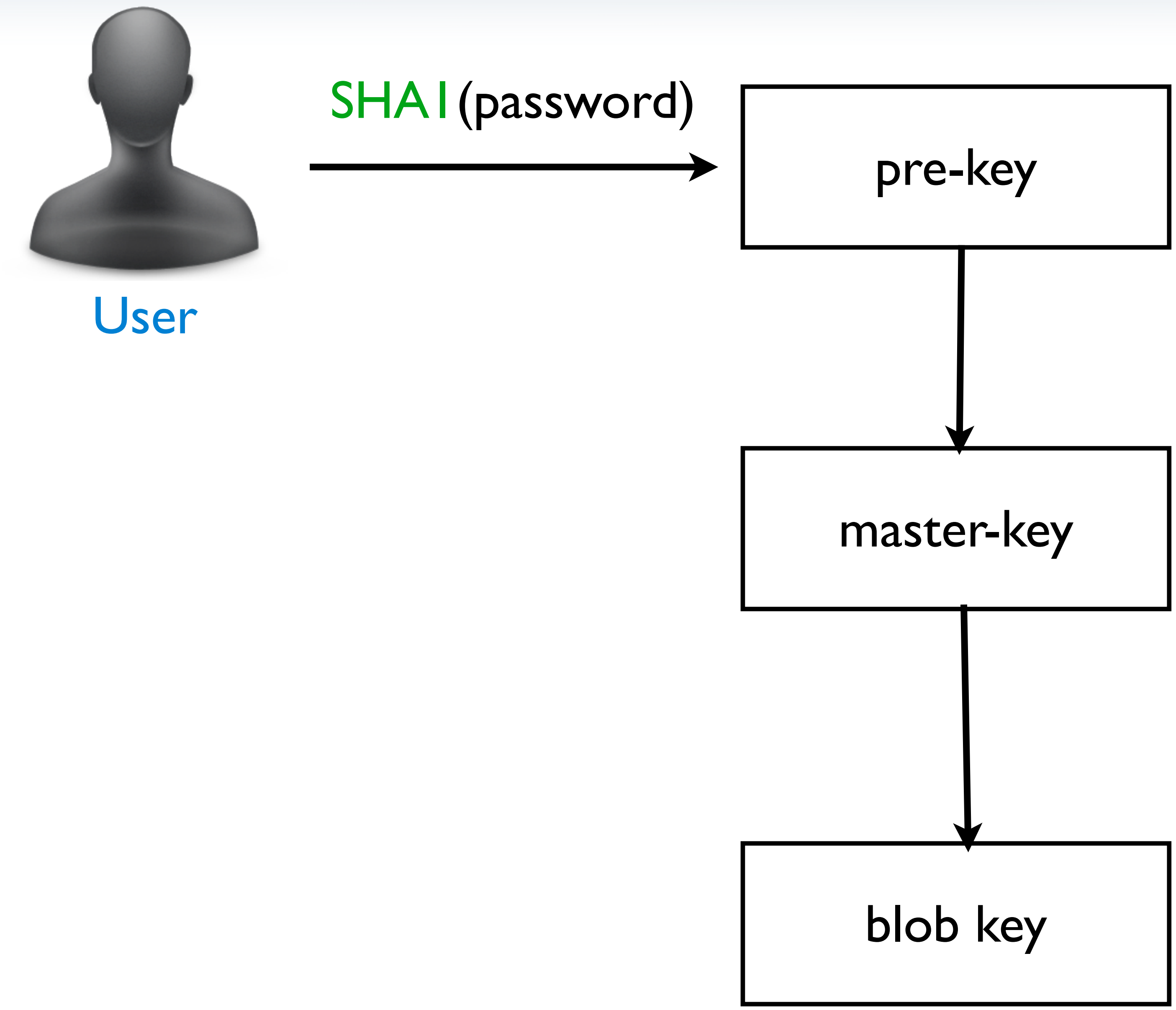
SHA1(password)

pre-key

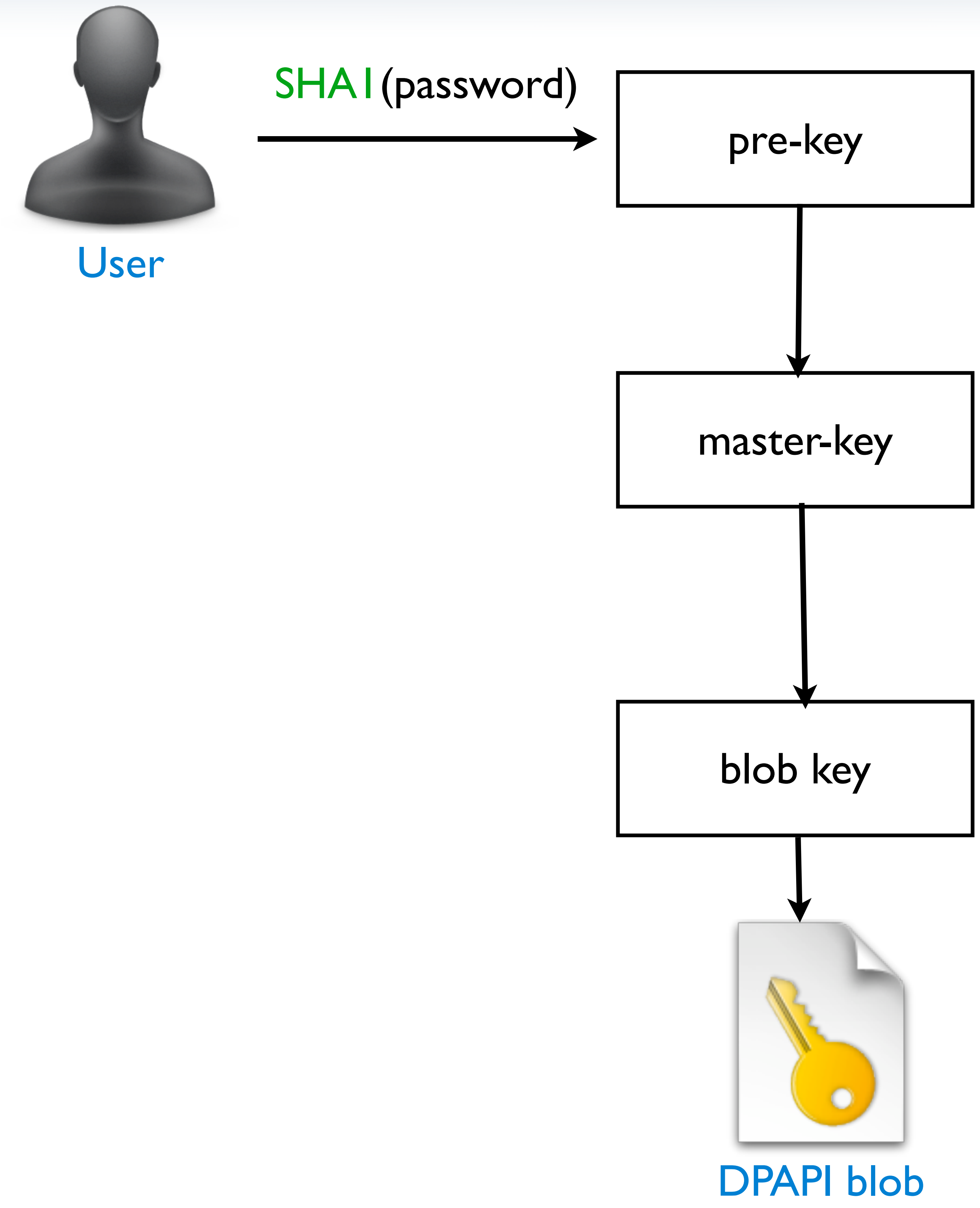
DPAPI derivation scheme



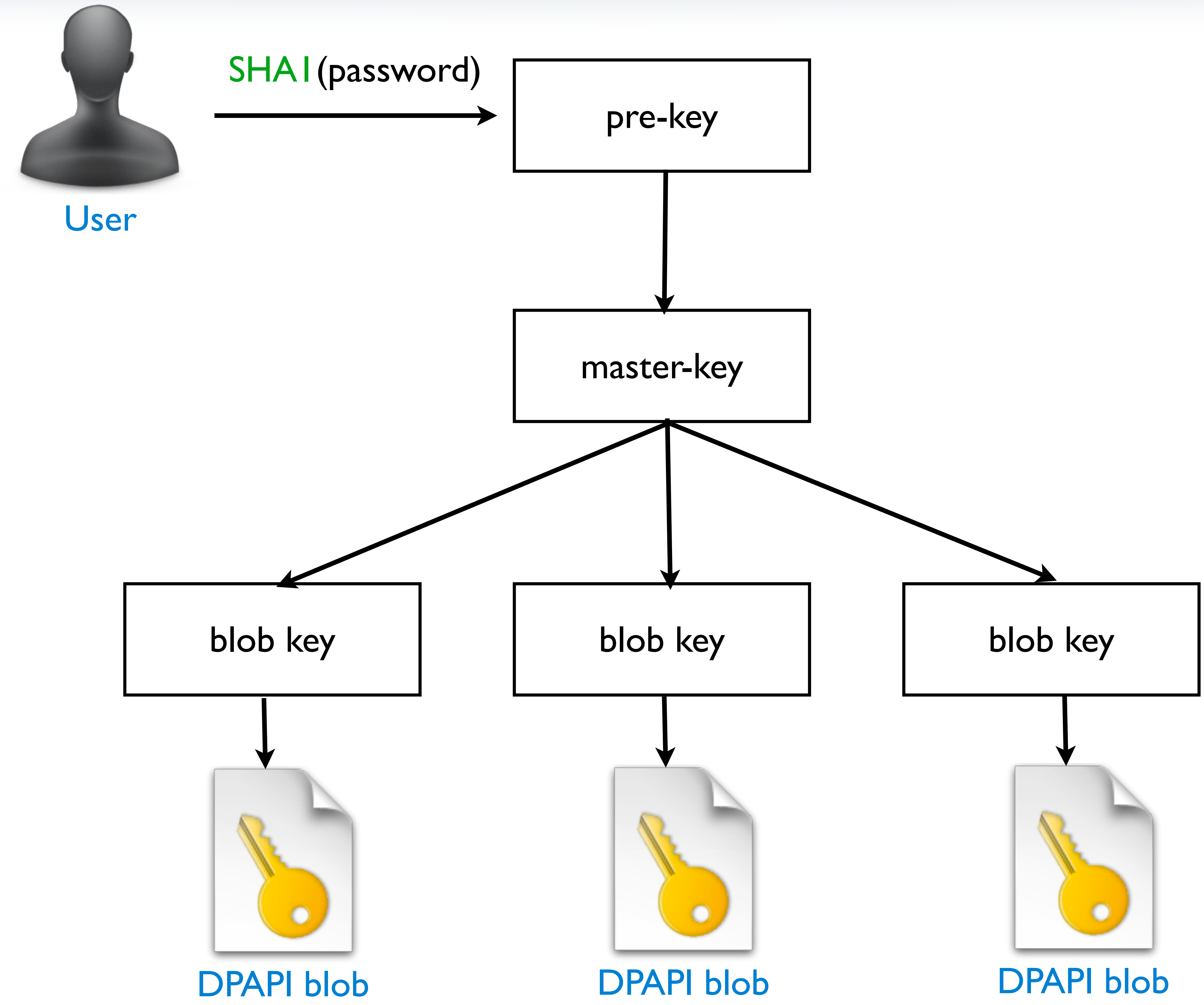
DPAPI derivation scheme



DPAPI derivation scheme



DPAPI derivation scheme



DPAPI Blob structure

```
struct wincrypt_datablob {
   DWORD   cbProviders,
   GUID    pbProviders[cbProviders],
   DWORD   cbMasterkeys,
   GUID    pbMasterkeys[cbMasterkeys],
   DWORD   dwFlags,
   DWORD   cbDescription,
   BYTE    pbDescription[cbDescription],
   ALG_ID  algCipher,
   DWORD   cbKey,
   DWORD   cbData,
   BYTE    pbData[cbData],
   DWORD   dwUnknown,
   ALG_ID  algHash,
   DWORD   dwHashSize,
   DWORD   cbSalt,
   BYTE    pbSalt[cbSalt],
   DWORD   cbCipher,
   BYTE    pbCipher[cbCipher],
   DWORD   cbCrc,
   BYTE    pbCrc[cbCrc]
}  ;
```

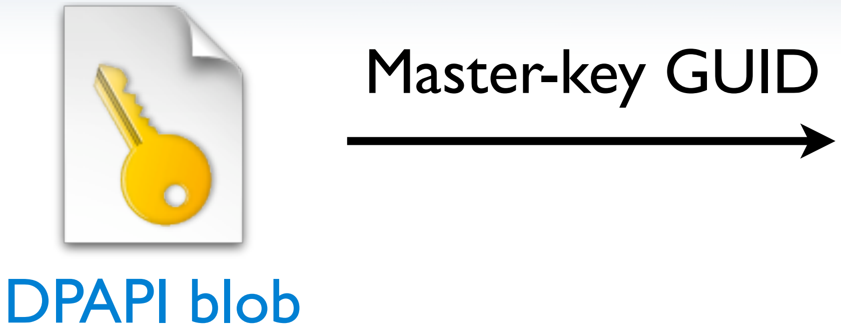
DPAPI master-key structure

Header Structure

```
struct wincrypt_masterkey_masterkeybloc
{
  DWORD   dwRevision,
  BYTE    pbSalt[16],
  DWORD   dwRounds,
  ALG_ID  algMAC,
  ALG_ID  algCipher,
  BYTE    pbEncrypted[]
};
```

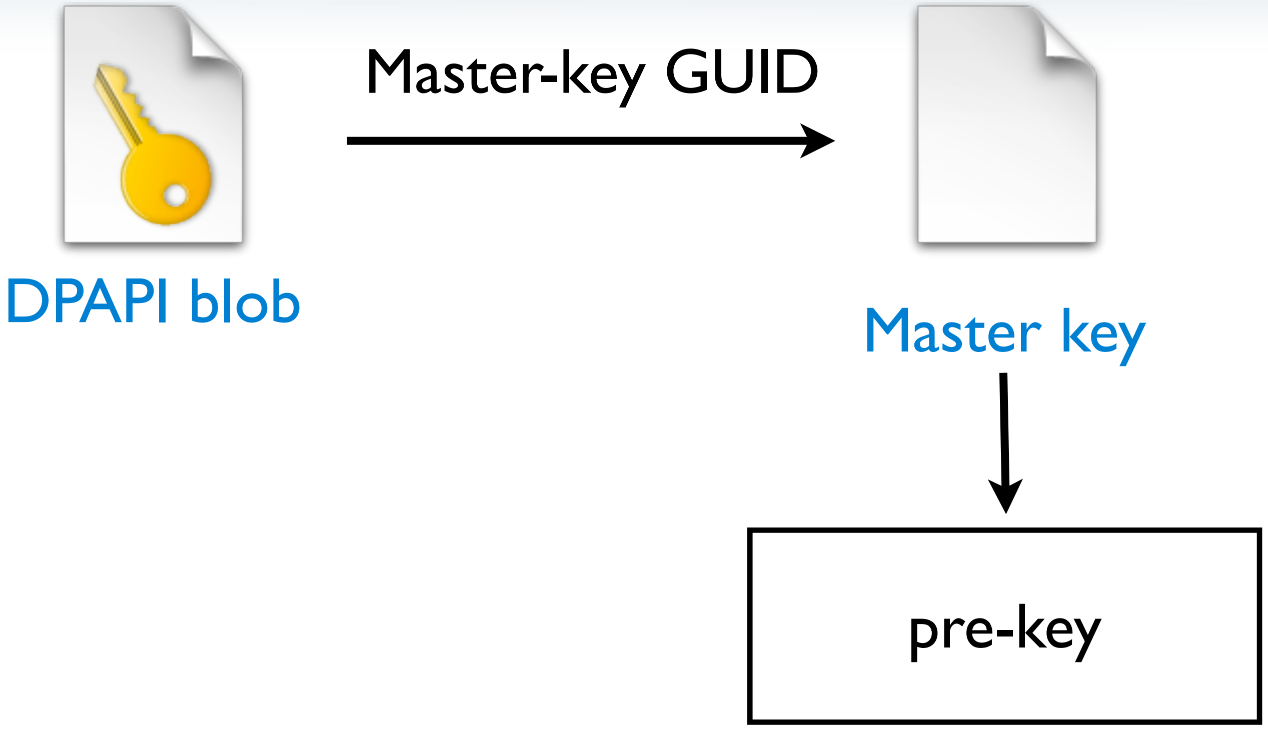
Footer Structure

DPAPI blob



Master-key GUID

DPAPI blob

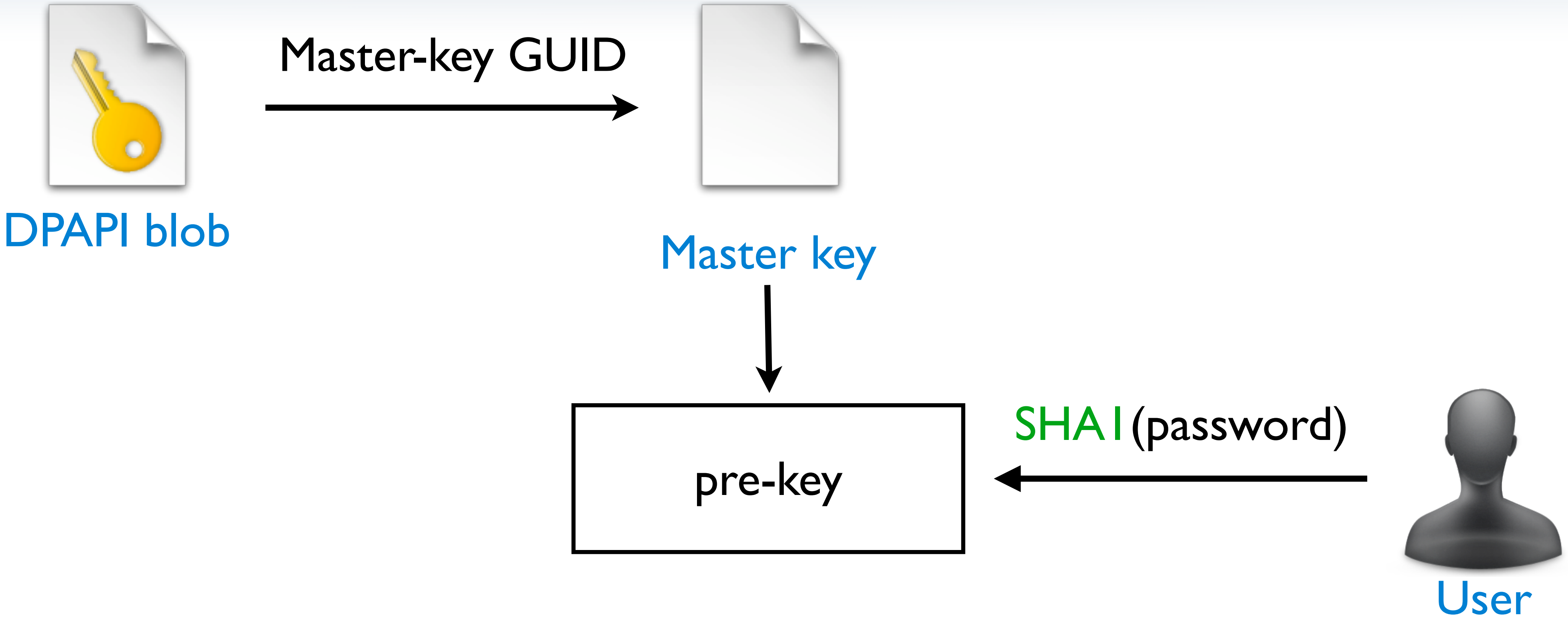


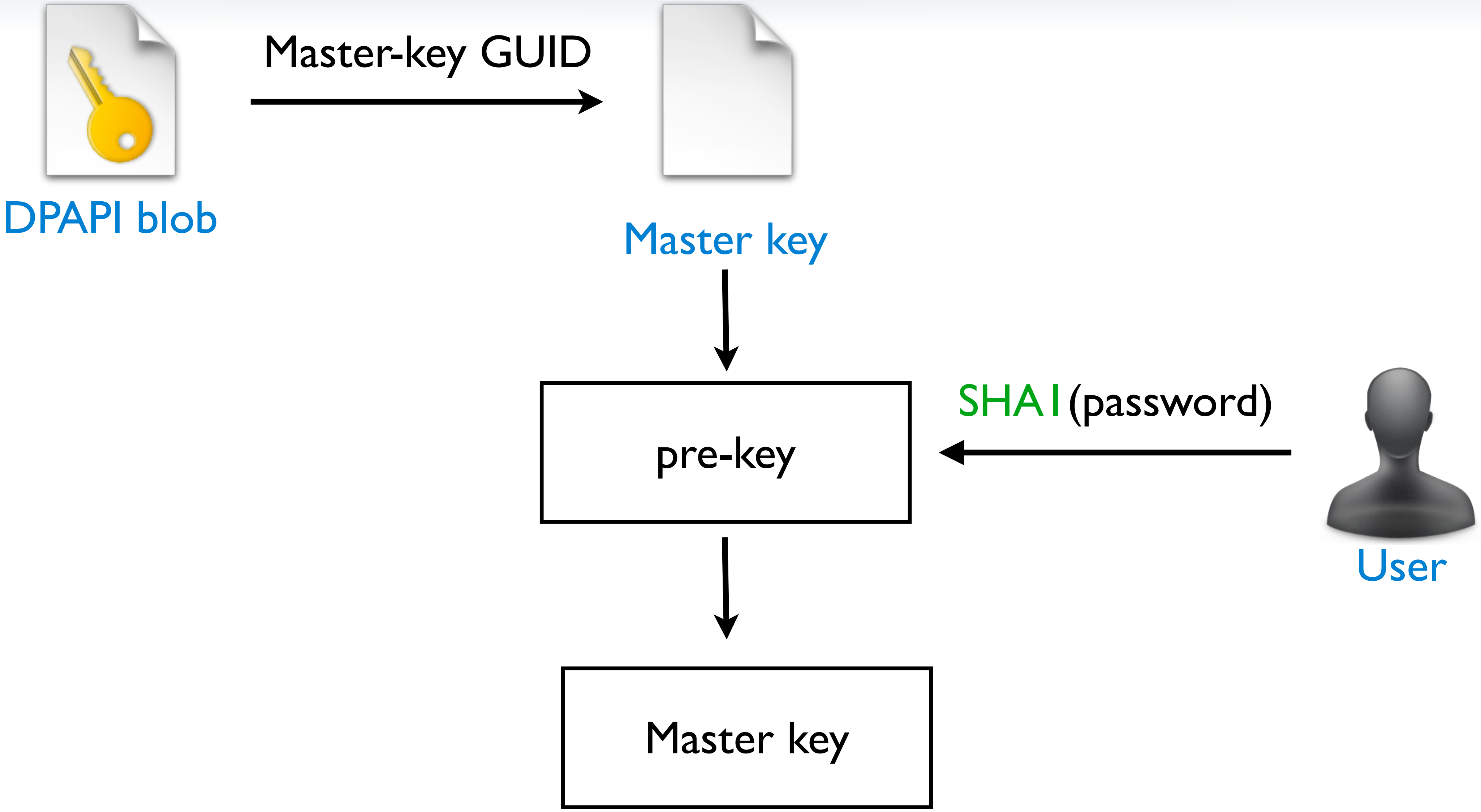
DPAPI blob

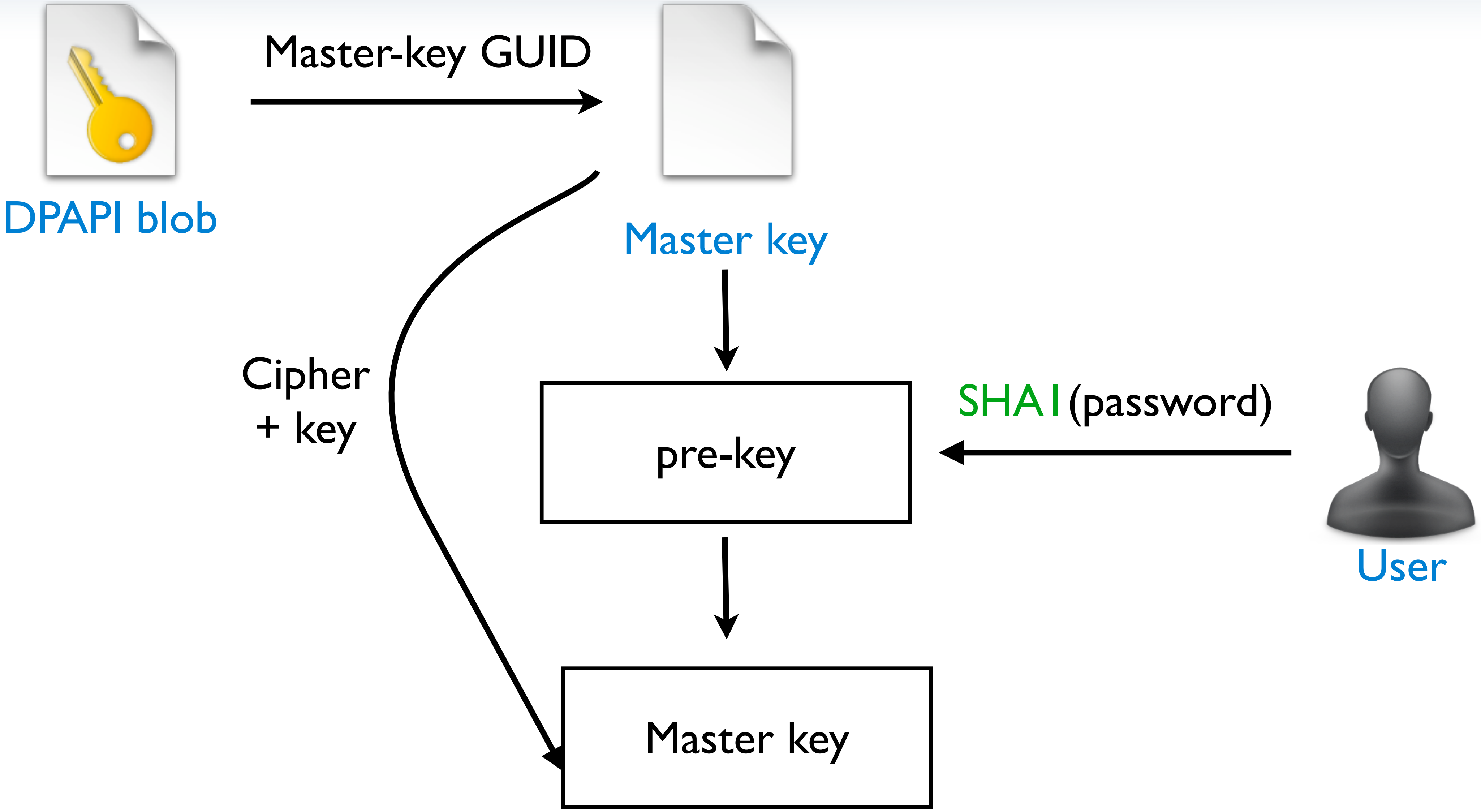
Master-key GUID

Master key

pre-key


Master-key GUID
DPAPI blob
Master key
pre-key
SHA1(password)
User


Master-key GUID
DPAPI blob
Master key
SHA1(password)
pre-key
User
Master key



Master-key GUID

DPAPI blob

Master key

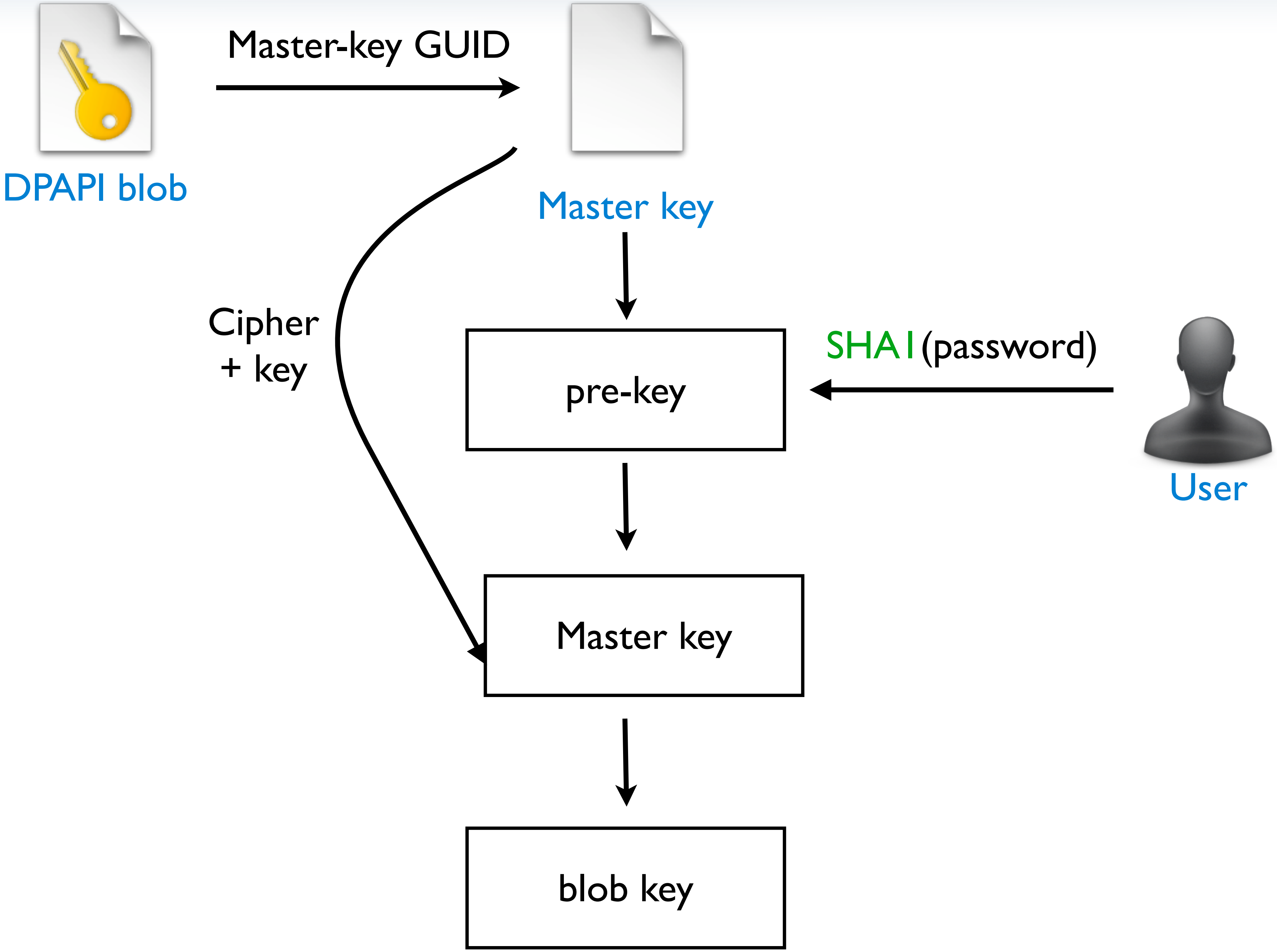
Cipher
+ key

pre-key

SHA1(password)

User

Master key



DPAPI blob

Master-key GUID

Master key

Cipher + key

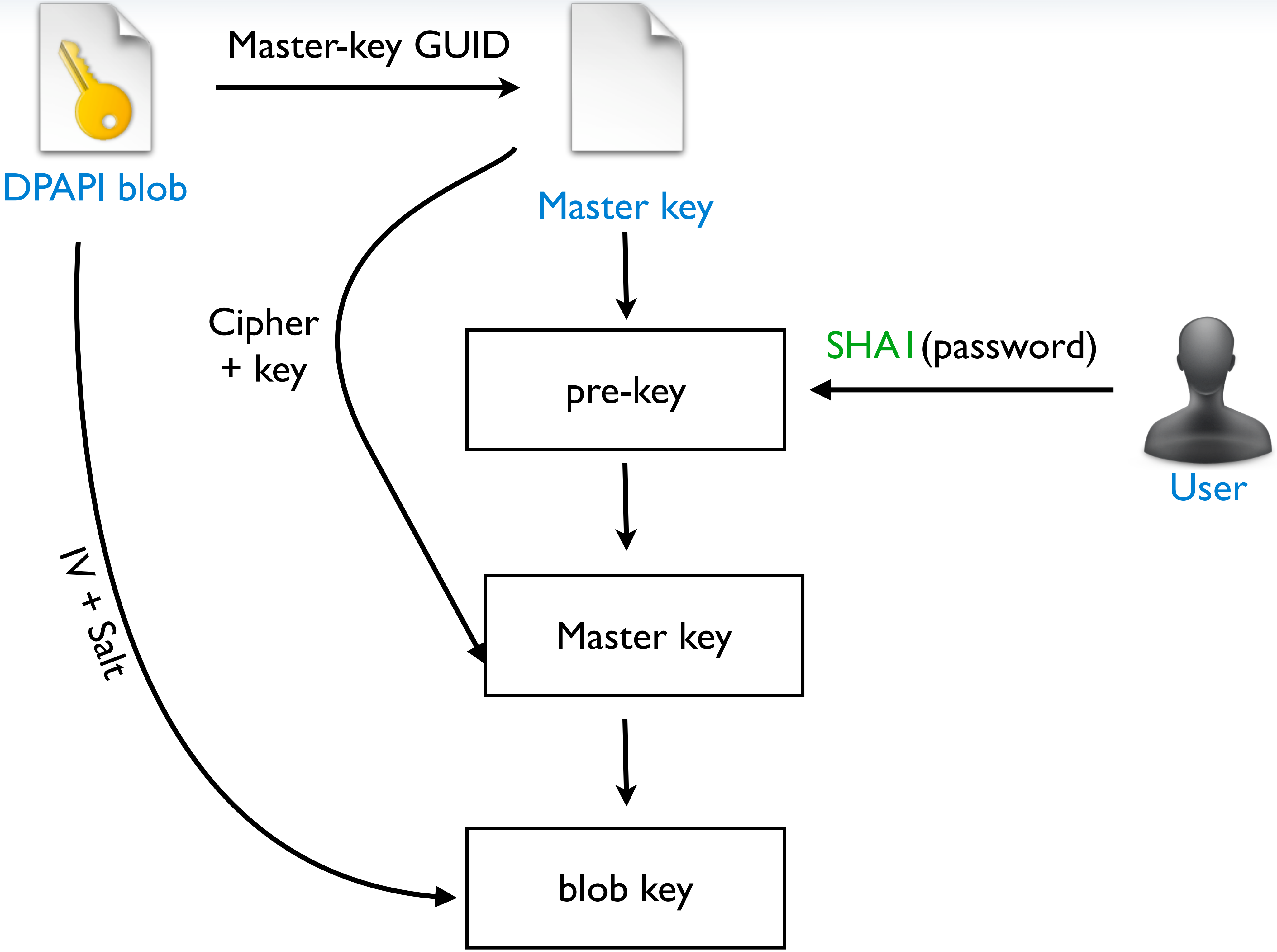
pre-key

SHA1(password)

User

Master key

blob key



DPAPI blob

Master-key GUID

Master key

Cipher
+ key

IV + Salt

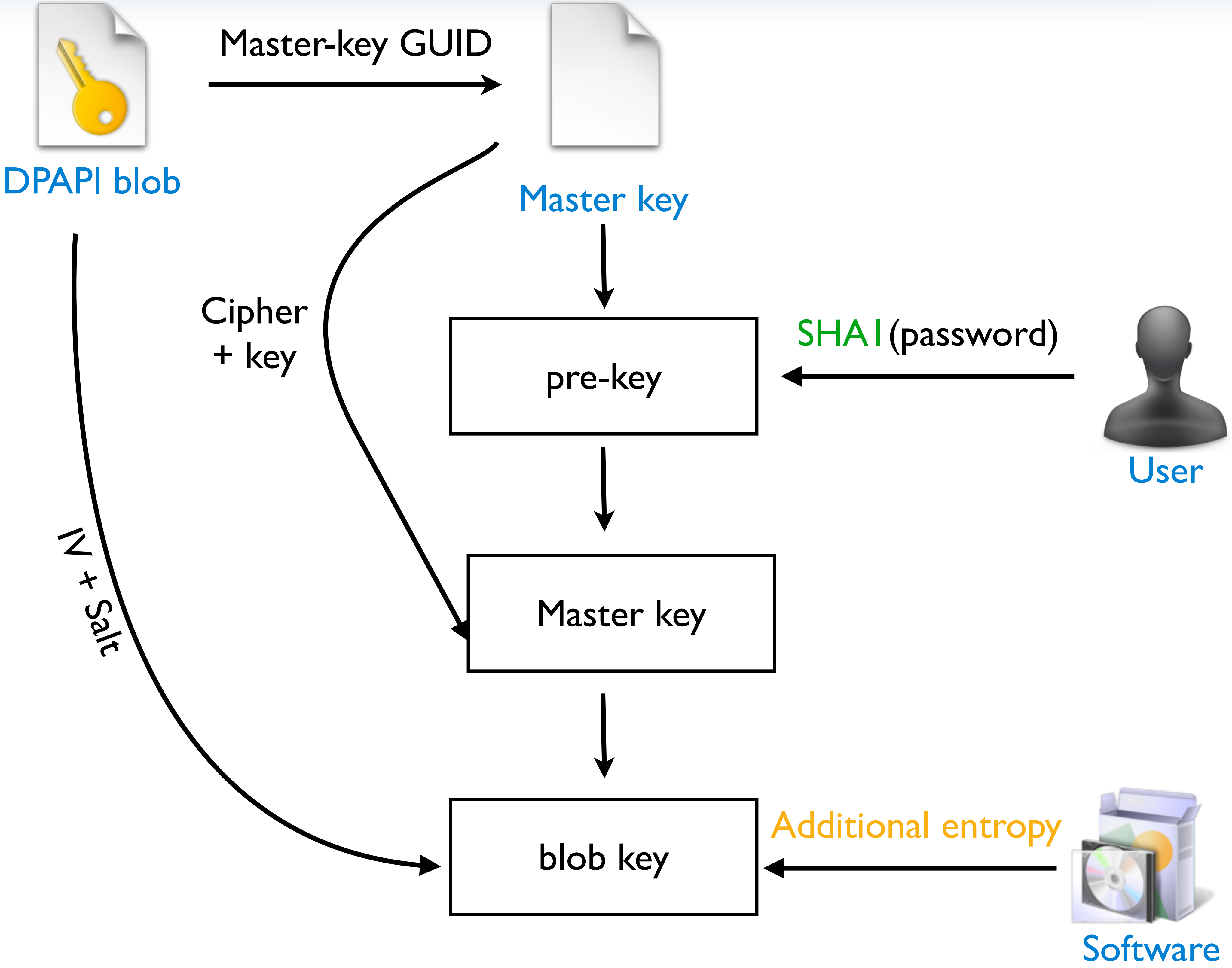
pre-key

SHA1(password)

User

Master key

blob key


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

DPAPI additional entropy

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

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 uses Moonsols to recover it

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)
  - Key (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...

Decrypting WiFi password

- Use a LSASecret as DPAPI key
- Array of credentials
  - HelpAssistant password in clear
  - DPAPI_SYSTEM
- “Encrypted”

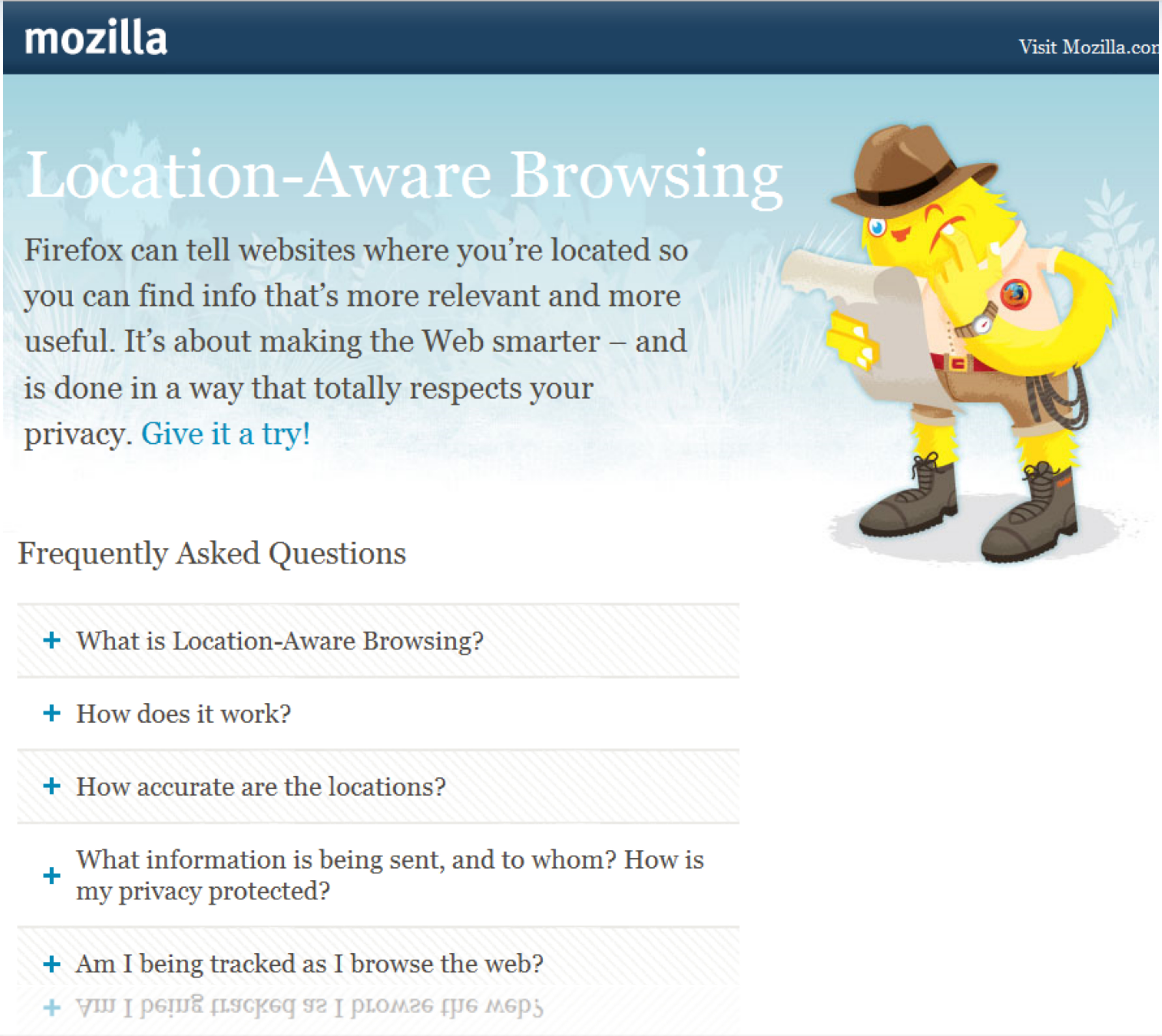
Where are you ?

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

Where are you ?

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

HTML5 Geo-location protocol



mozilla

Visit Mozilla.cor

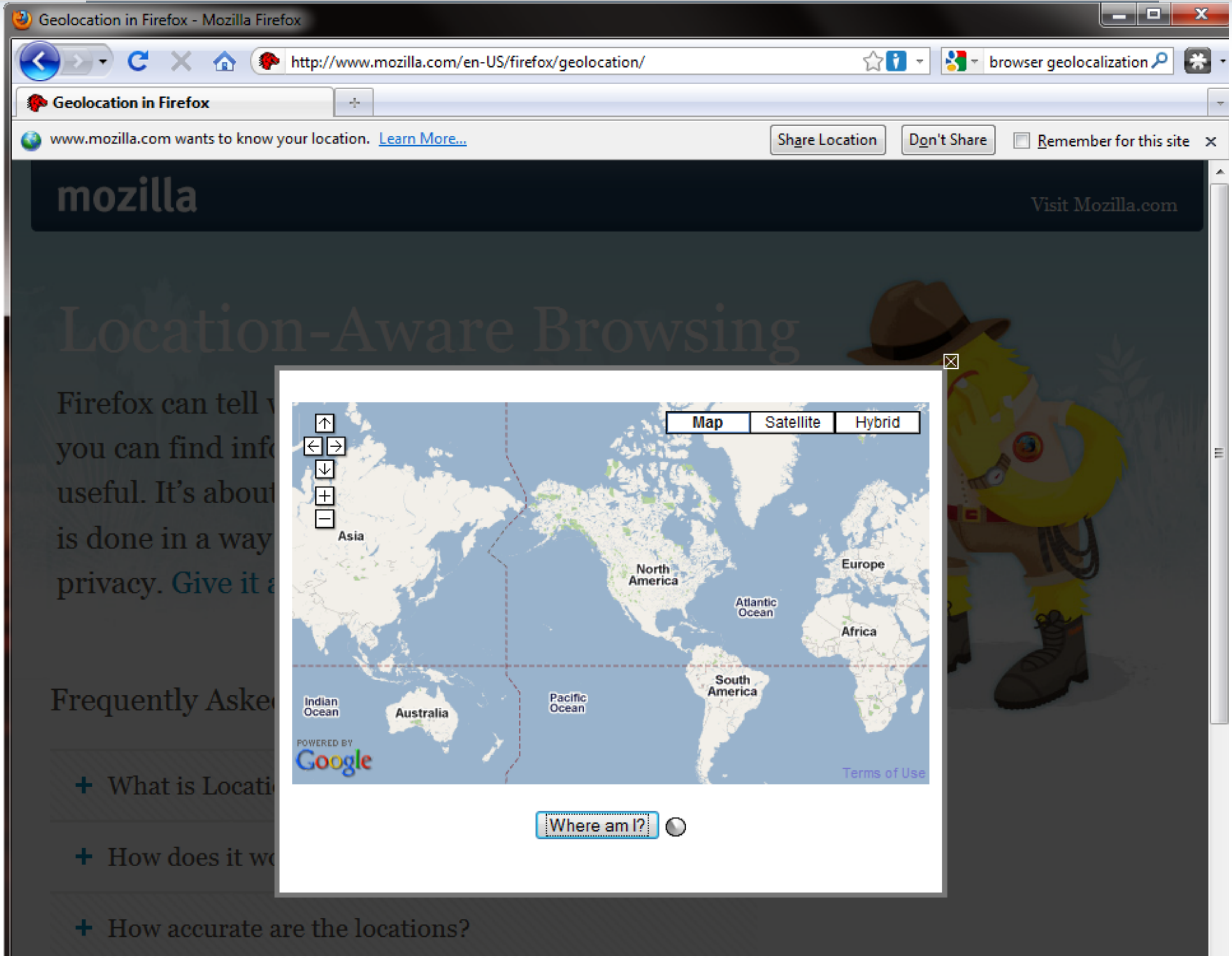
Location-Aware Browsing

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/

browser geolocalization

Geolocation in Firefox

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

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

mozilla

Visit Mozilla.com

Location-Aware Browsing

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

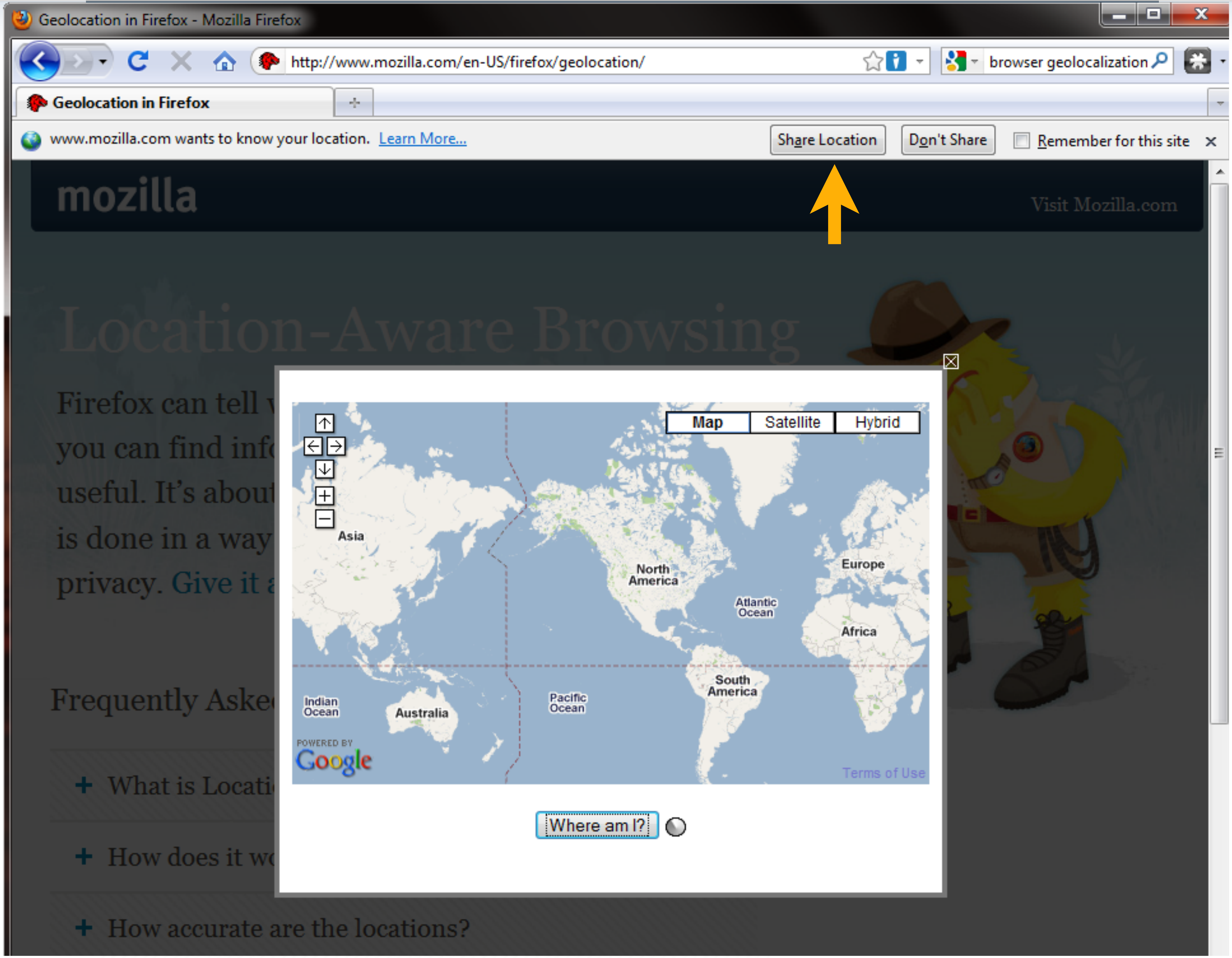
Frequently Aske

+ 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/

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

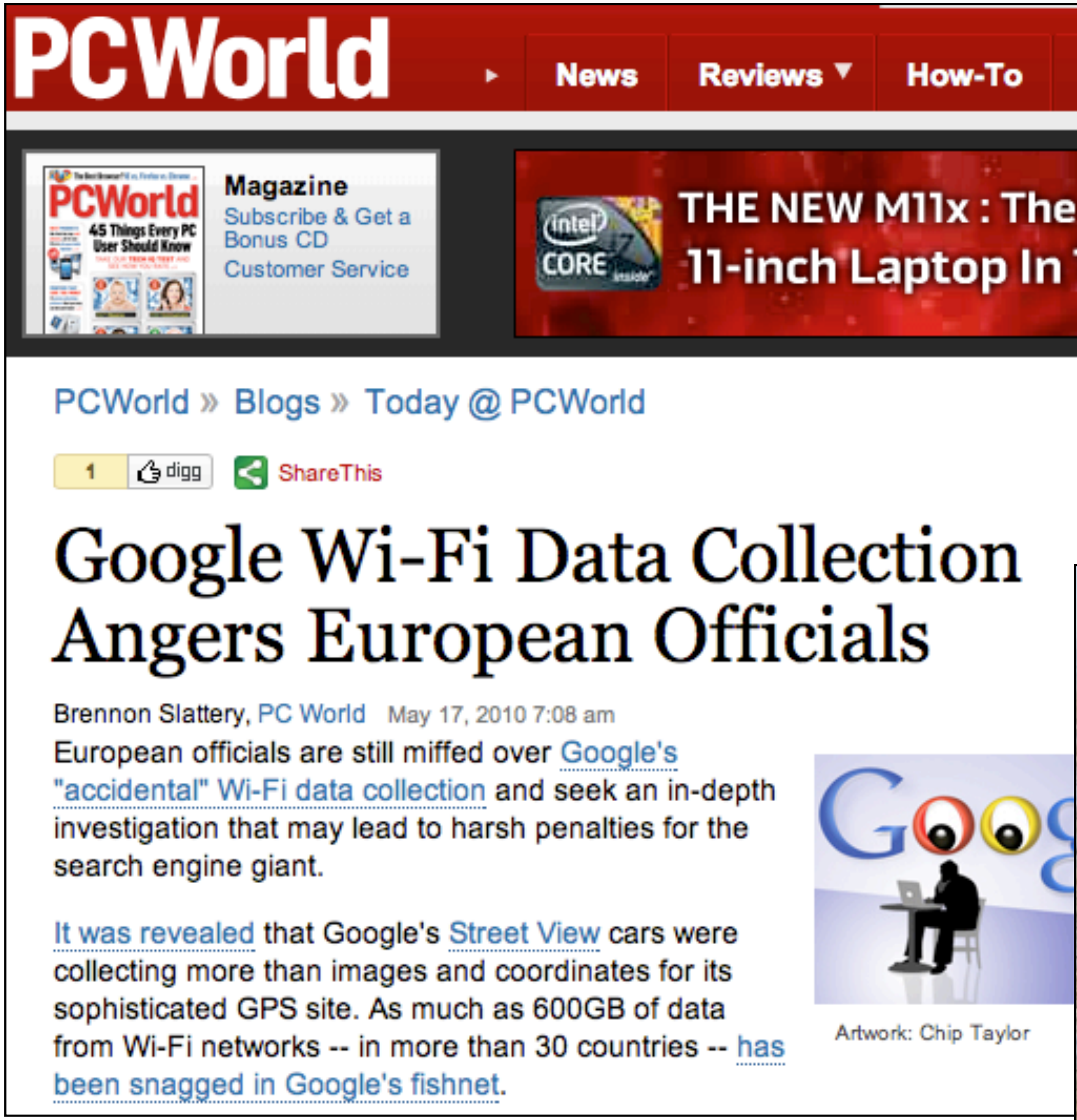
Location-Aware Browsing

Firefox can tell w
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 wo
+ How accurate are the locations?

Behind the curtain



PCWorld ▸ News Reviews ▾ How-To Download

PCWorld 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

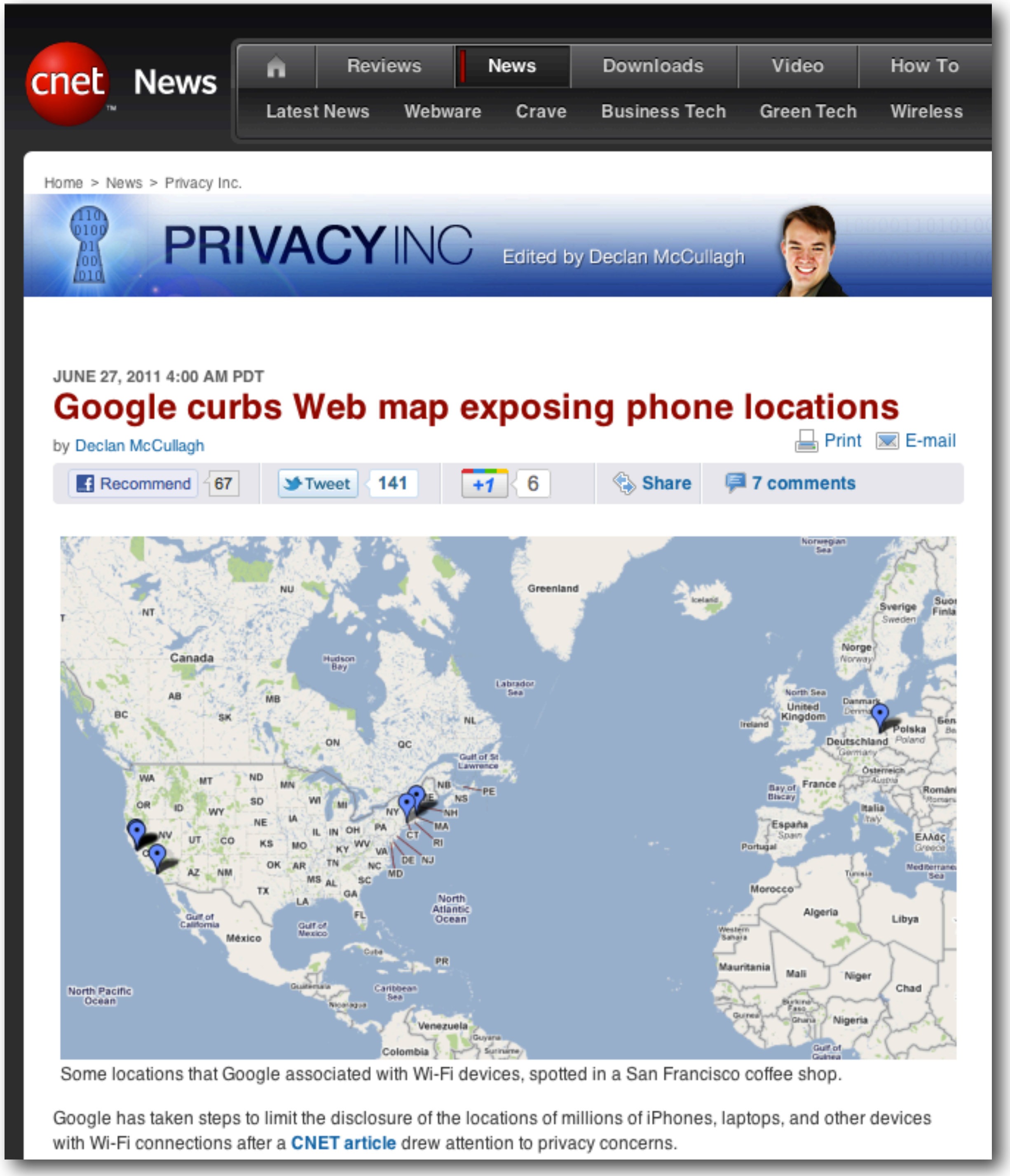
European officials are still miffed over Google's "accidental" Wi-Fi data collection and seek an in-depth investigation that may lead to harsh penalties for the search engine giant.

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
- So we started to look for 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.

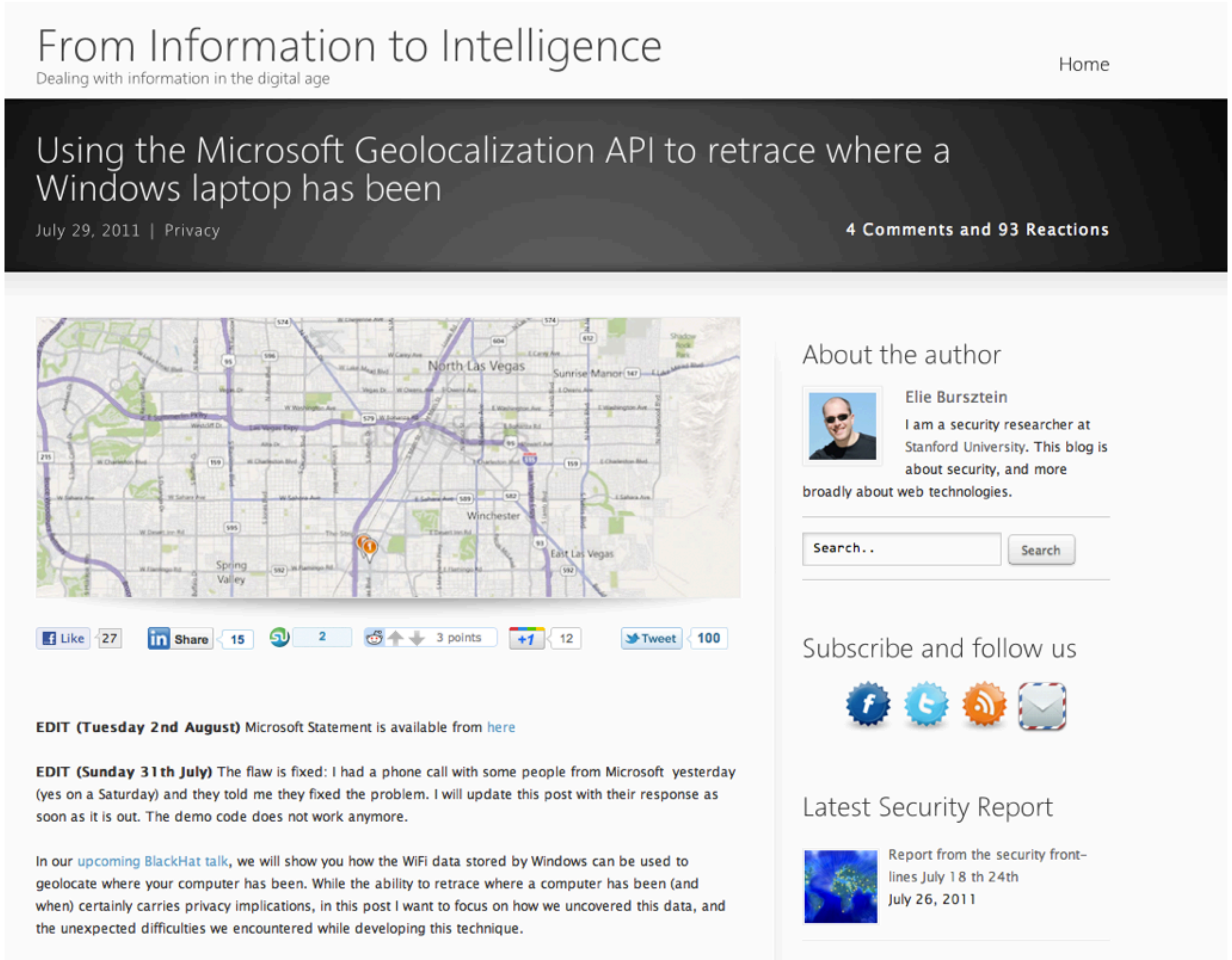
Google has taken steps to limit the disclosure of the locations of millions of iPhones, laptops, and other devices with Wi-Fi connections after a **CNET article** drew attention to privacy concerns.

Entering Microsoft

- Live service
- “Documented” in the Windows mobile MSDN
- After sniffing the traffic:
  - Use a big SOAP request
  - Does not check any ID fields
  - Allows to supply one MAC

```
<GetLocationUsingFingerprint xmlns="http://
inference.location.live.com">
     <RequestHeader>
        <Timestamp>2011-02-15T16:22:47.0000968-05:00
          </Timestamp>
        <ApplicationId>e1e71f6b-2149-45f3-b298-a20XXXXX5017
          </ApplicationId>
        <TrackingId>21BF9AD6-CFD3-46B2-B042-EE90XXXXXX
          </TrackingId>
       <DeviceProfile ClientGuid="0fc571be-4622-4ce0-b04e-
     XXXXXXeb1a222" Platform="Windows7" DeviceType="PC"
     OSVersion="7600.16695.amd64fre.win7_gdr.101026-1503"
     LFVersion="9.0.8080.16413" ExtendedDeviceInfo="" />
      <Authorization />
  </RequestHeader>
  <BeaconFingerprint>
  <Detections>
    <Wifi7 BssId="00:BA:DC:0F:FE:00" rssi="-25" />
  </Detections>
  </BeaconFingerprint>
 </GetLocationUsingFingerprint>
```

Blog post and demo released !



From Information to Intelligence

Dealing with information in the digital age

Home

Using the Microsoft Geolocalization API to retrace where a Windows laptop has been

July 29, 2011 | Privacy

4 Comments and 93 Reactions

EDIT (Tuesday 2nd August) Microsoft Statement is available from here

EDIT (Sunday 31th July) The flaw is fixed: I had a phone call with some people from Microsoft yesterday (yes on a Saturday) and they told me they fixed the problem. I will update this post with their response as soon as it is out. The demo code does not work anymore.

In our upcoming BlackHat talk, we will show you how the WiFi data stored by Windows can be used to geolocate where your computer has been. While the ability to retrace where a computer has been (and when) certainly carries privacy implications, in this post I want to focus on how we uncovered this data, and the unexpected difficulties we encountered while developing this technique.

About the author

Elie Bursztein

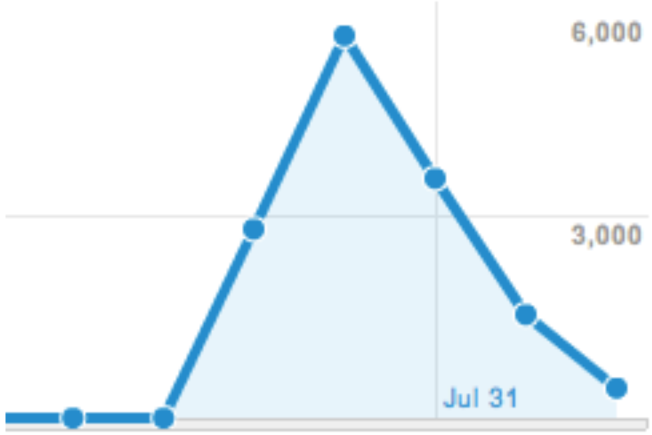
I am a security researcher at Stanford University. This blog is about security, and more broadly about web technologies.

Subscribe and follow us

Latest Security Report

Report from the security front-lines July 18 th 24th

July 26, 2011



13,188 people visited this site

13,963 Visits

13,188 Unique Visitors

51,805 Pageviews

3.71 Pages/Visit

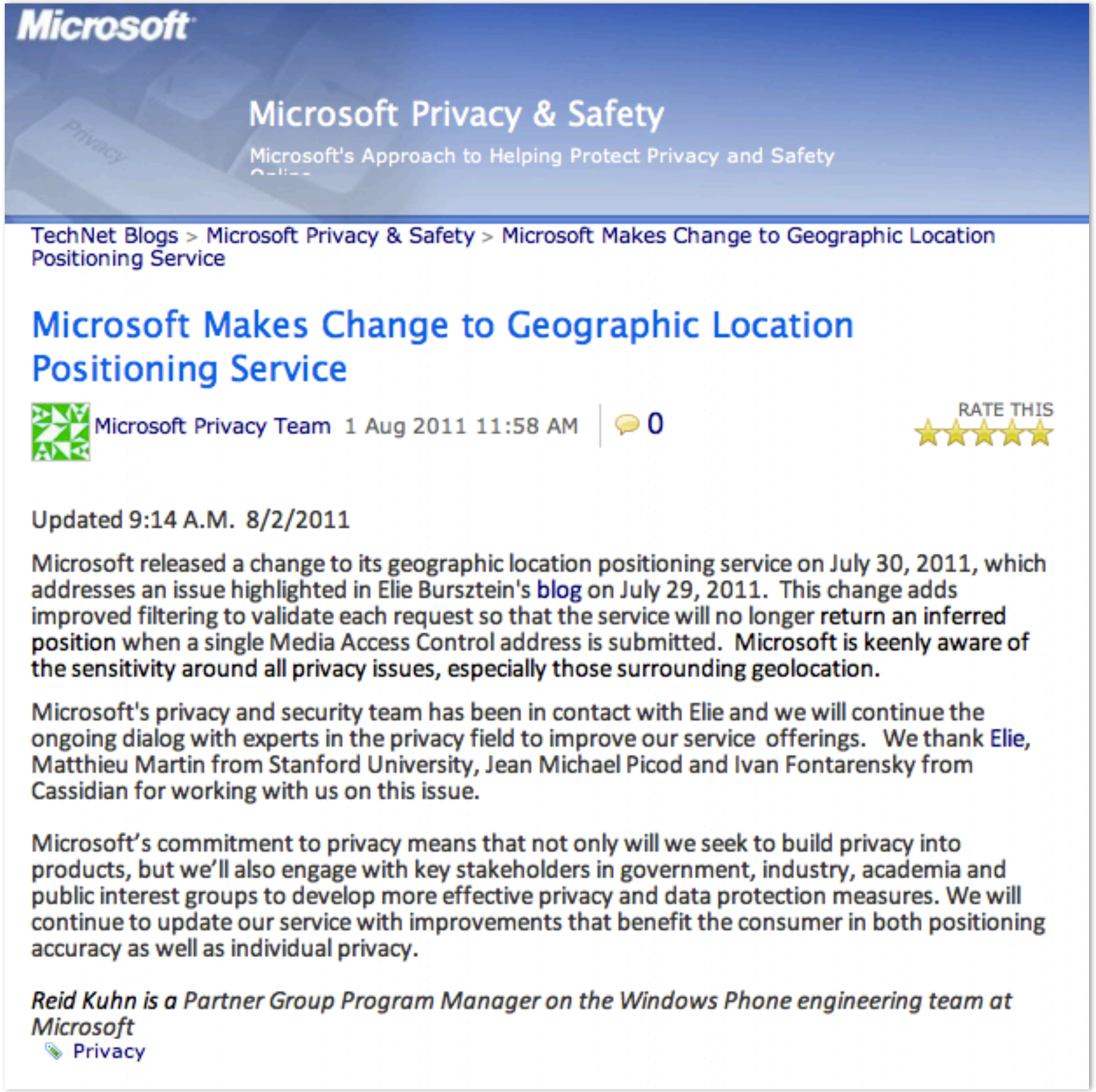
00:02:04 Avg. Time on Site

22.94% Bounce Rate

94.13% % New Visits

Fixed just before the Blackhat

- Fixed last weekend
- No longer return location for a single address


Microsoft
Microsoft Privacy & Safety
Microsoft's Approach to Helping Protect Privacy and Safety Online

TechNet Blogs > Microsoft Privacy & Safety > Microsoft Makes Change to Geographic Location Positioning Service

Microsoft Makes Change to Geographic Location Positioning Service

Microsoft Privacy Team 1 Aug 2011 11:58 AM | 0 RATE THIS

Updated 9:14 A.M. 8/2/2011

Microsoft released a change to its geographic location positioning service on July 30, 2011, which addresses an issue highlighted in Elie Bursztein's blog on July 29, 2011. This change adds improved filtering to validate each request so that the service will no longer return an inferred position when a single Media Access Control address is submitted. Microsoft is keenly aware of the sensitivity around all privacy issues, especially those surrounding geolocation.

Microsoft's privacy and security team has been in contact with Elie and we will continue the ongoing dialog with experts in the privacy field to improve our service offerings. We thank Elie, Matthieu Martin from Stanford University, Jean Michael Picod and Ivan Fontarensky from Cassidian for working with us on this issue.

Microsoft's commitment to privacy means that not only will we seek to build privacy into products, but we'll also engage with key stakeholders in government, industry, academia and public interest groups to develop more effective privacy and data protection measures. We will continue to update our service with improvements that benefit the consumer in both positioning accuracy as well as individual privacy.

Reid Kuhn is a Partner Group Program Manager on the Windows Phone engineering team at Microsoft

Privacy

Geo-location API restrictions

Google™

Requires 2 MAC close from each other

SKYHOOK WIRELESS

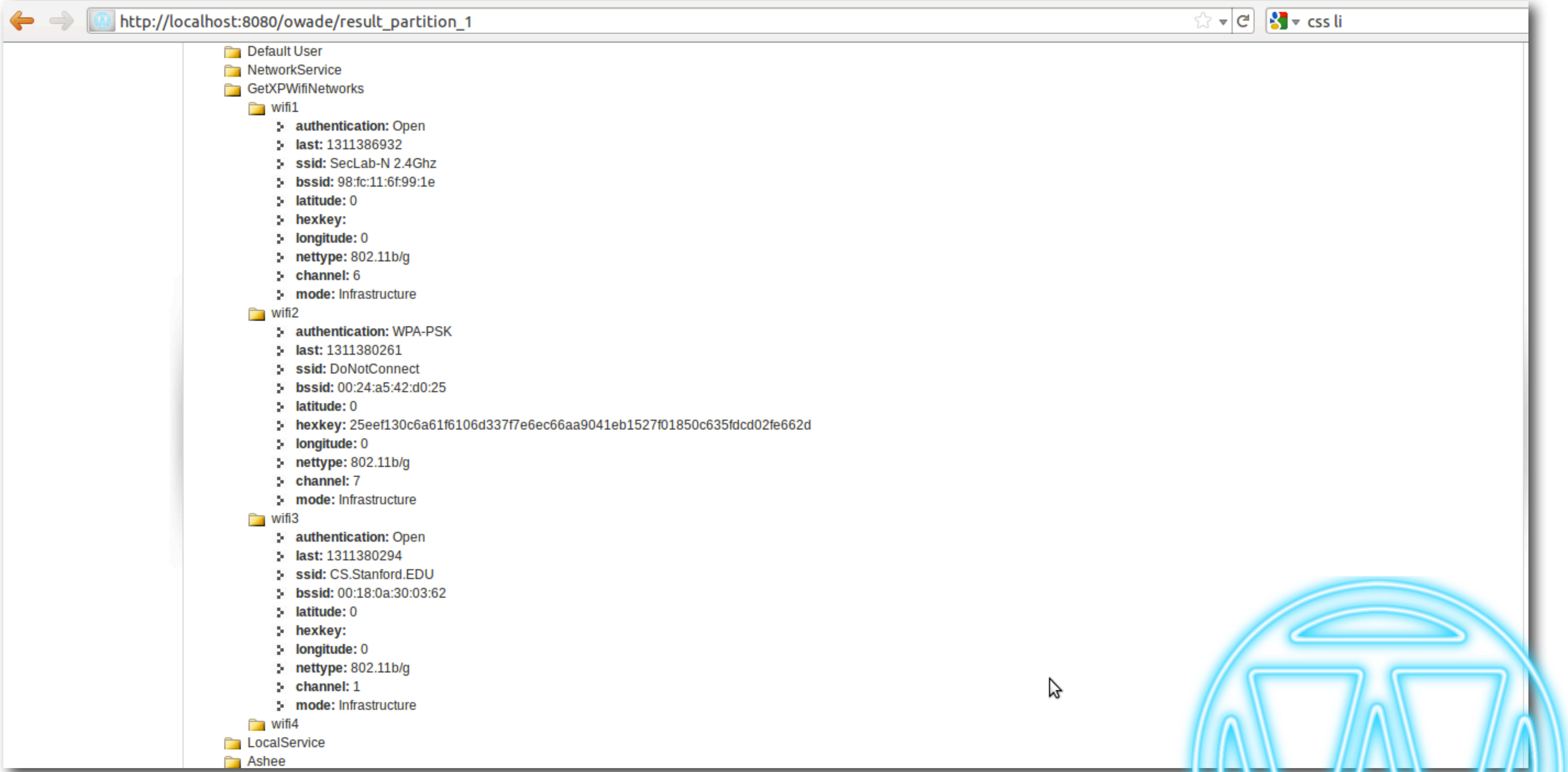
The MAC and IP location need to be “close”

Microsoft®

Requires multiples MAC addresses

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

WiFi Information Extracted By OWDE



- Default User
- NetworkService
- GetXPWifiNetworks
  - wifi1
    - **authentication:** Open
    - **last:** 1311386932
    - **ssid:** SecLab-N 2.4Ghz
    - **bssid:** 98:fc:11:6f:99:1e
    - **latitude:** 0
    - **hexkey:**
    - **longitude:** 0
    - **nettype:** 802.11b/g
    - **channel:** 6
    - **mode:** Infrastructure
  - wifi2
    - **authentication:** WPA-PSK
    - **last:** 1311380261
    - **ssid:** DoNotConnect
    - **bssid:** 00:24:a5:42:d0:25
    - **latitude:** 0
    - **hexkey:** 25eef130c6a61f6106d337f7e6ec66aa9041eb1527f01850c635fdcd02fe662d
    - **longitude:** 0
    - **nettype:** 802.11b/g
    - **channel:** 7
    - **mode:** Infrastructure
  - wifi3
    - **authentication:** Open
    - **last:** 1311380294
    - **ssid:** CS.Stanford.EDU
    - **bssid:** 00:18:0a:30:03:62
    - **latitude:** 0
    - **hexkey:**
    - **longitude:** 0
    - **nettype:** 802.11b/g
    - **channel:** 1
    - **mode:** Infrastructure
  - wifi4
- LocalService
- Ashee

Browsers

Firefox > 3.4

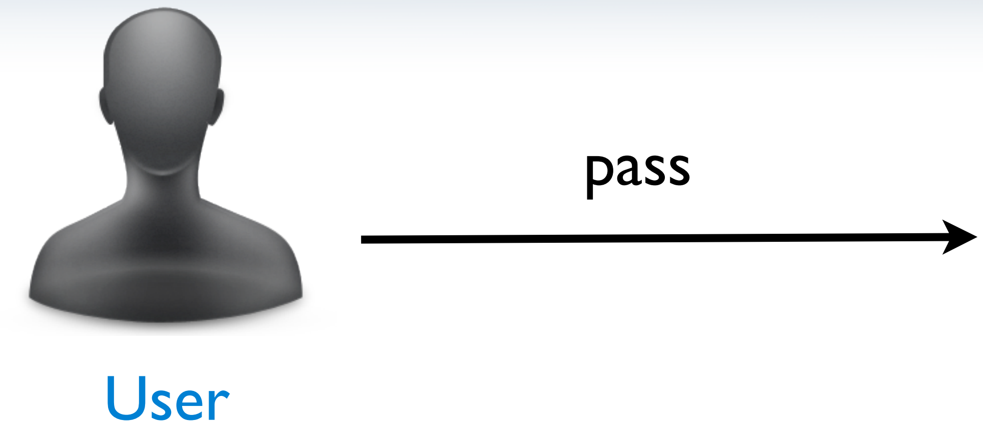
- Passwords
  - Location: signons.sqlite
  - Encryption: 3DES + Master password
- History
  - URLs: places.sqlite
  - Forms fields: formhistory.sqlite

Firefox

Take back the web

Decrypting Firefox password

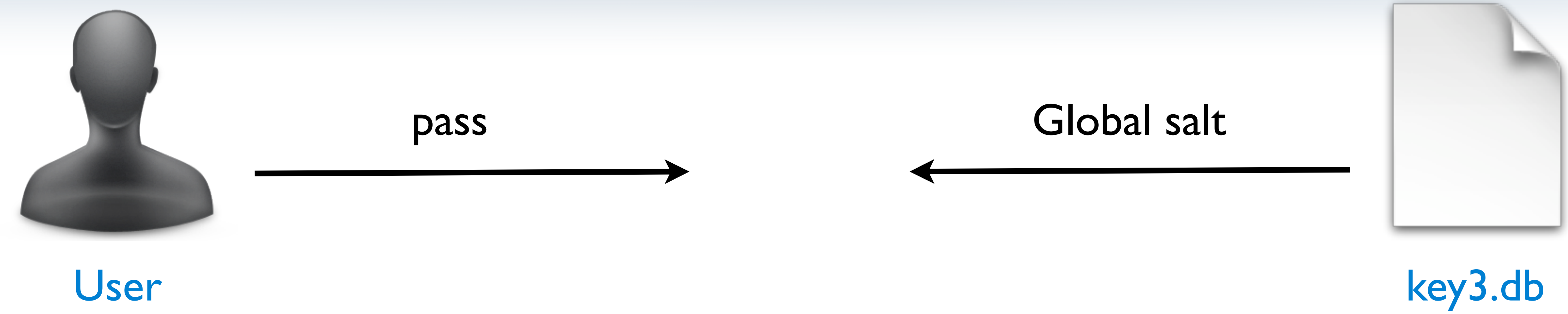
Decrypting Firefox password



pass

User

Decrypting Firefox password



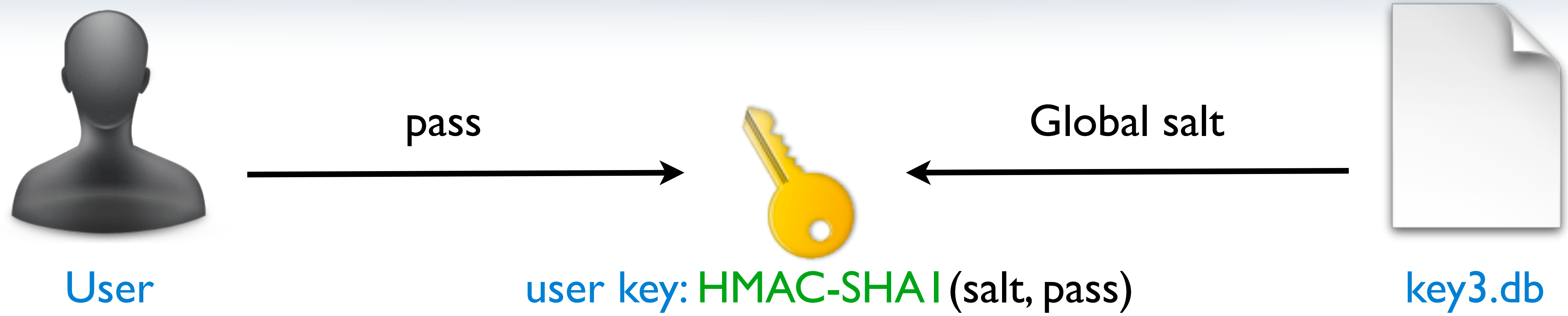
User

pass

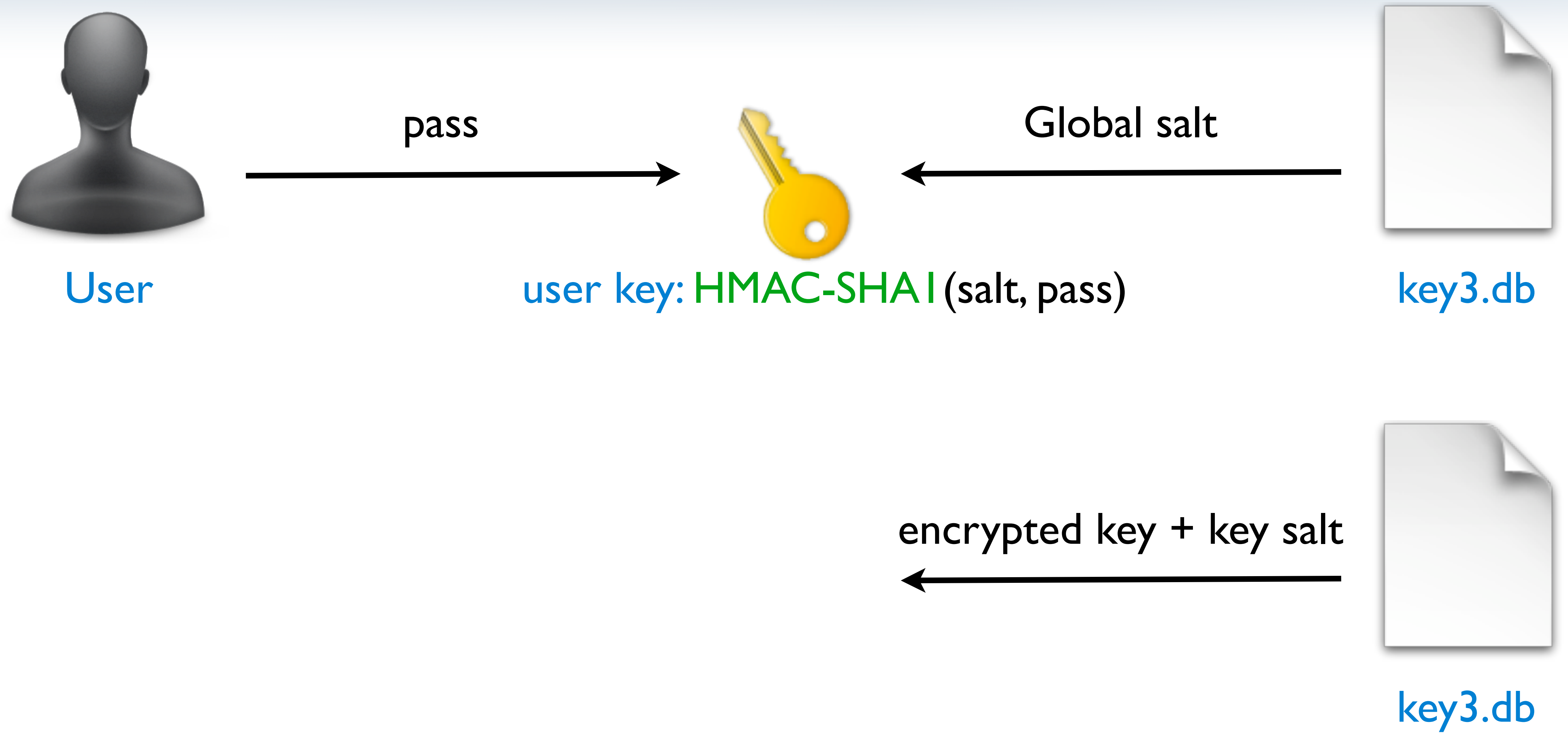
Global salt

key3.db

Decrypting Firefox password



Decrypting Firefox password



pass

Global salt

User

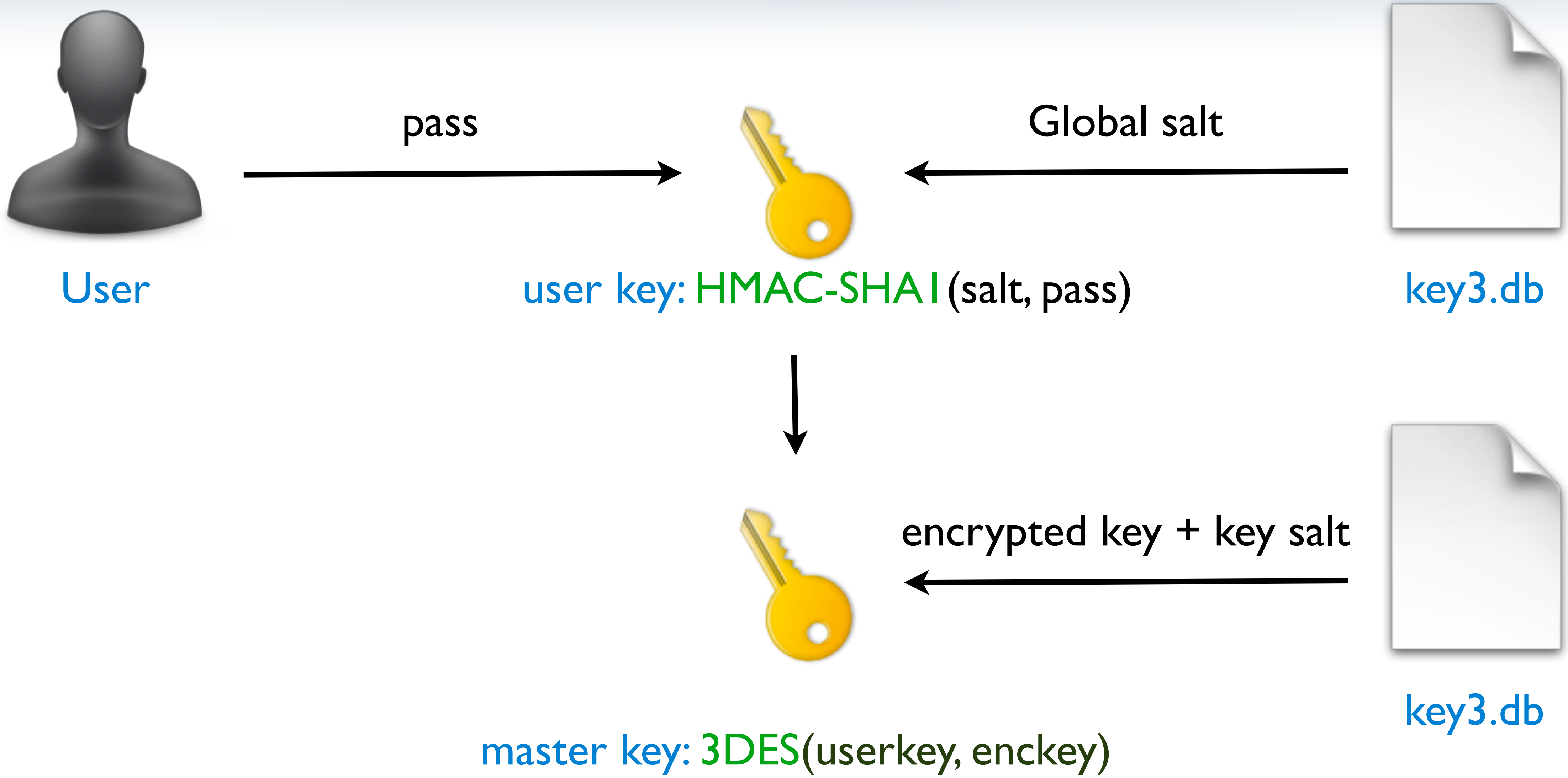
user key: HMAC-SHA1(salt, pass)

key3.db

encrypted key + key salt

key3.db

Decrypting Firefox password



User

pass

user key: HMAC-SHA1(salt, pass)

Global salt

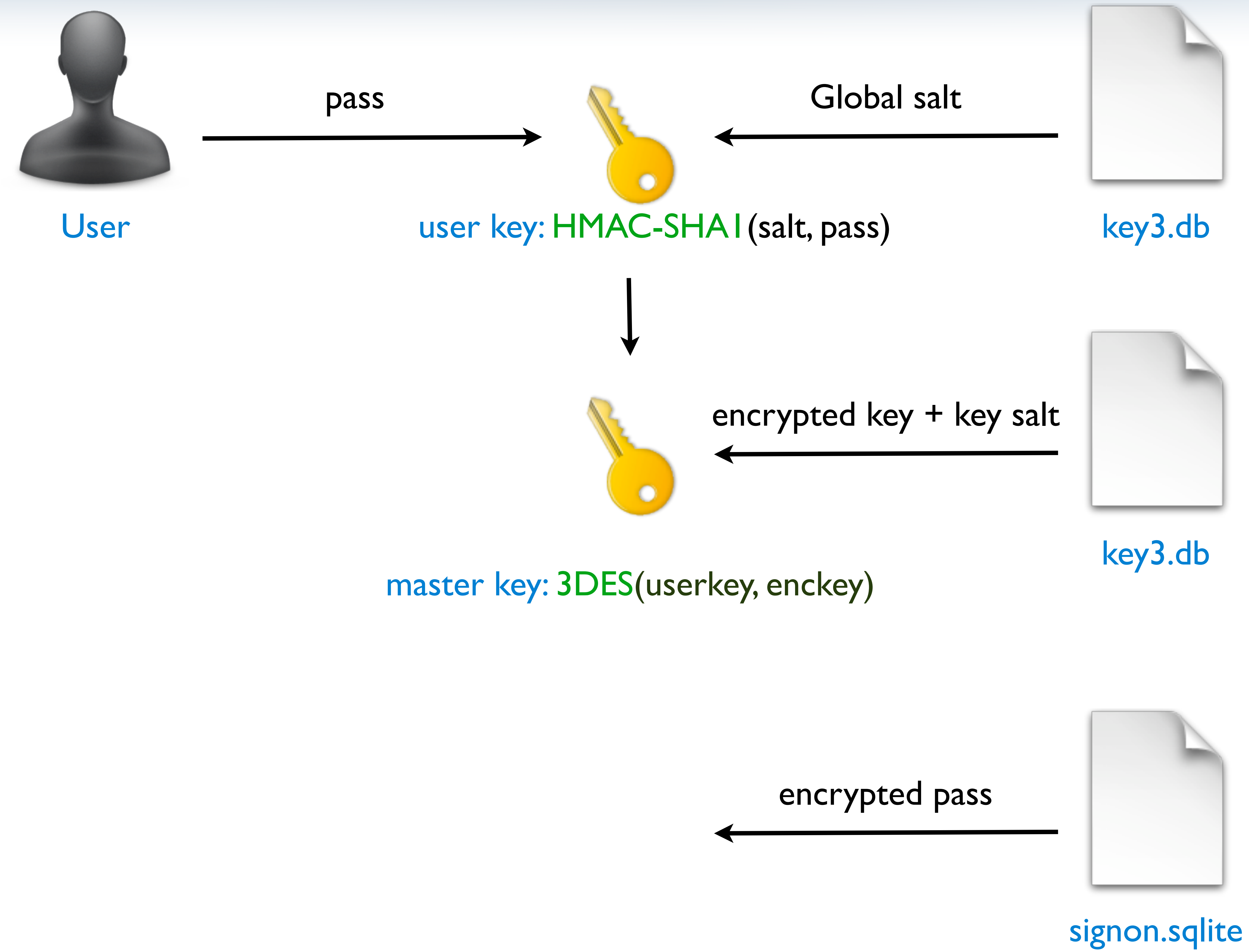
key3.db

encrypted key + key salt

key3.db

master key: 3DES(userkey, enckey)

Decrypting Firefox password



pass

Global salt

User

user key: HMAC-SHA1(salt, pass)

key3.db

encrypted key + key salt

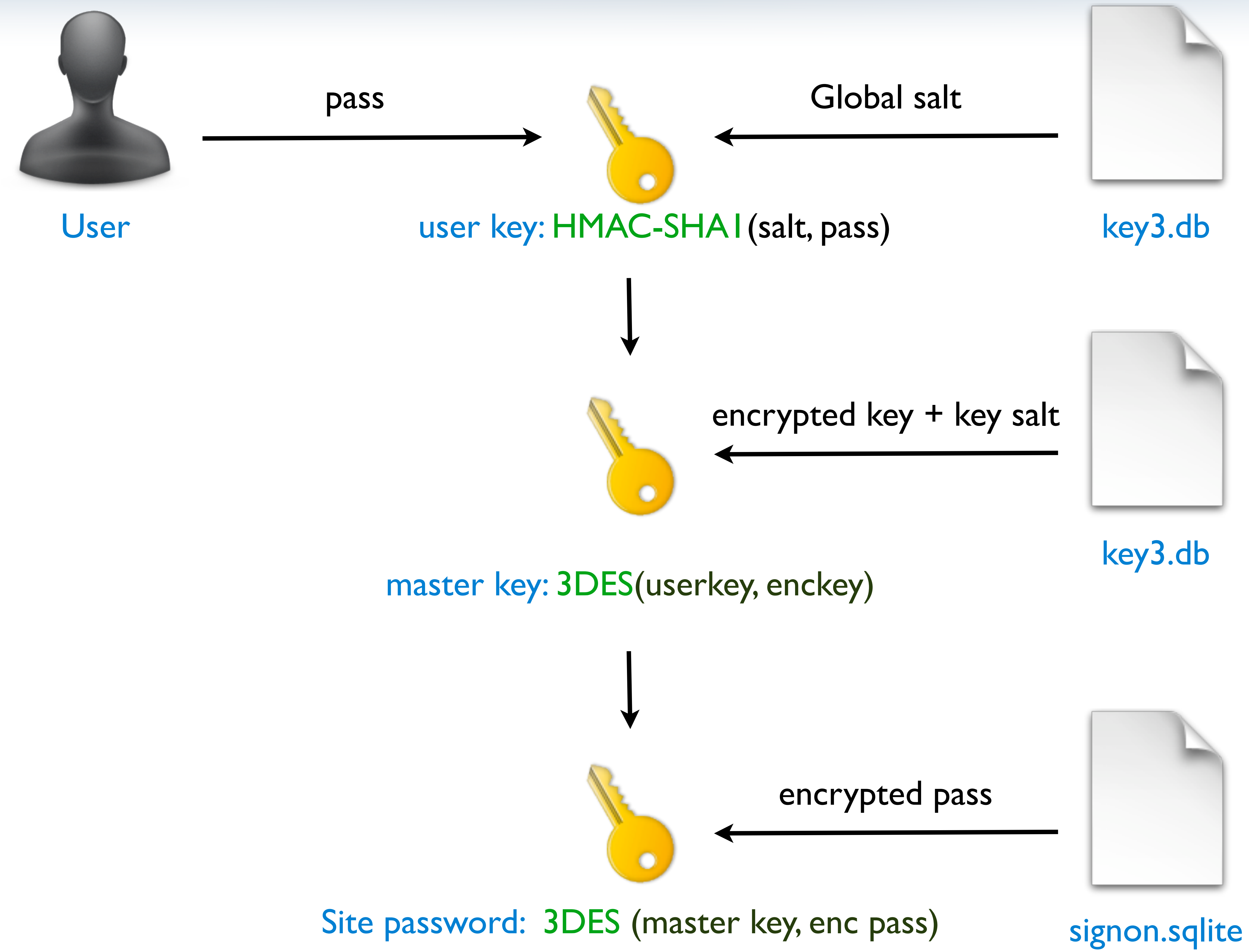
key3.db

master key: 3DES(userkey, enckey)

encrypted pass

signon.sqlite

Decrypting Firefox password



User

pass

Global salt

user key: HMAC-SHA1(salt, pass)

key3.db

encrypted key + key salt

key3.db

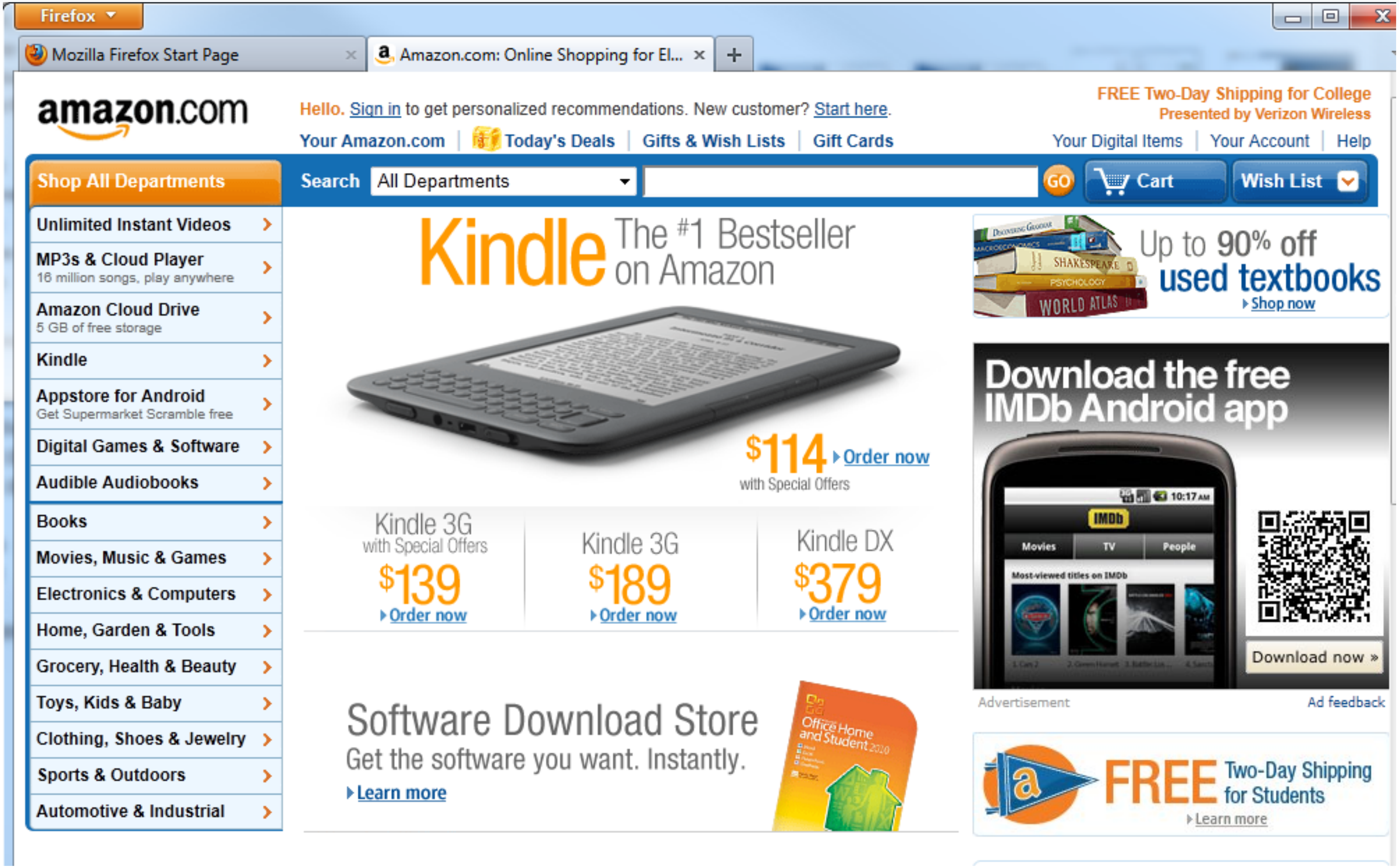
master key: 3DES(userkey, enckey)

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
$139
Order now

Kindle 3G
$189
Order now

Kindle DX
$379
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

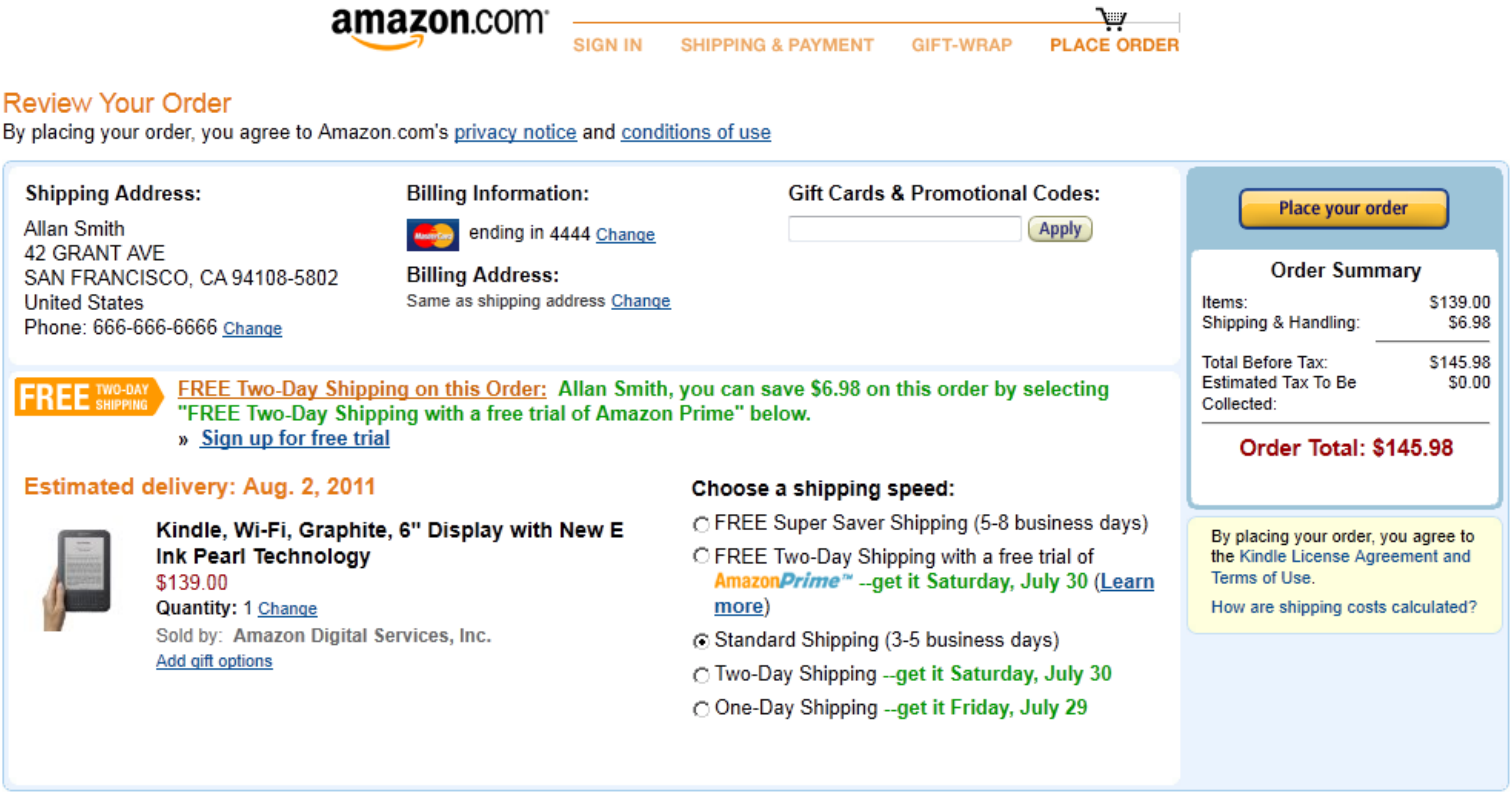
Download now »

Advertisement

Ad feedback

FREE Two-Day Shipping for Students
Learn more

How about a nice kindle ?



amazon.com

SIGN IN SHIPPING & PAYMENT GIFT-WRAP PLACE ORDER

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

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?

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

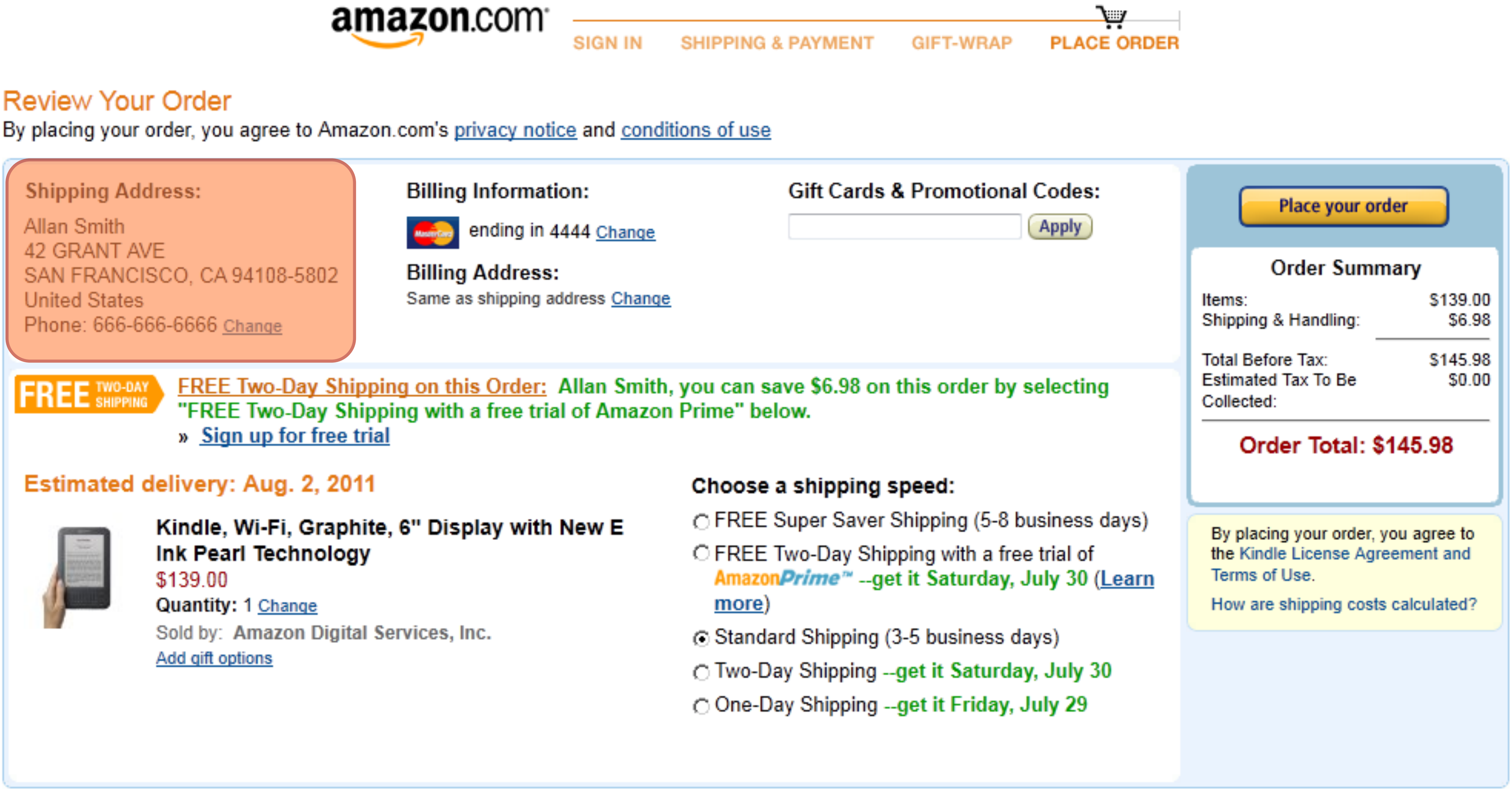
Estimated delivery: Aug. 2, 2011

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

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

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

How are shipping costs calculated?

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

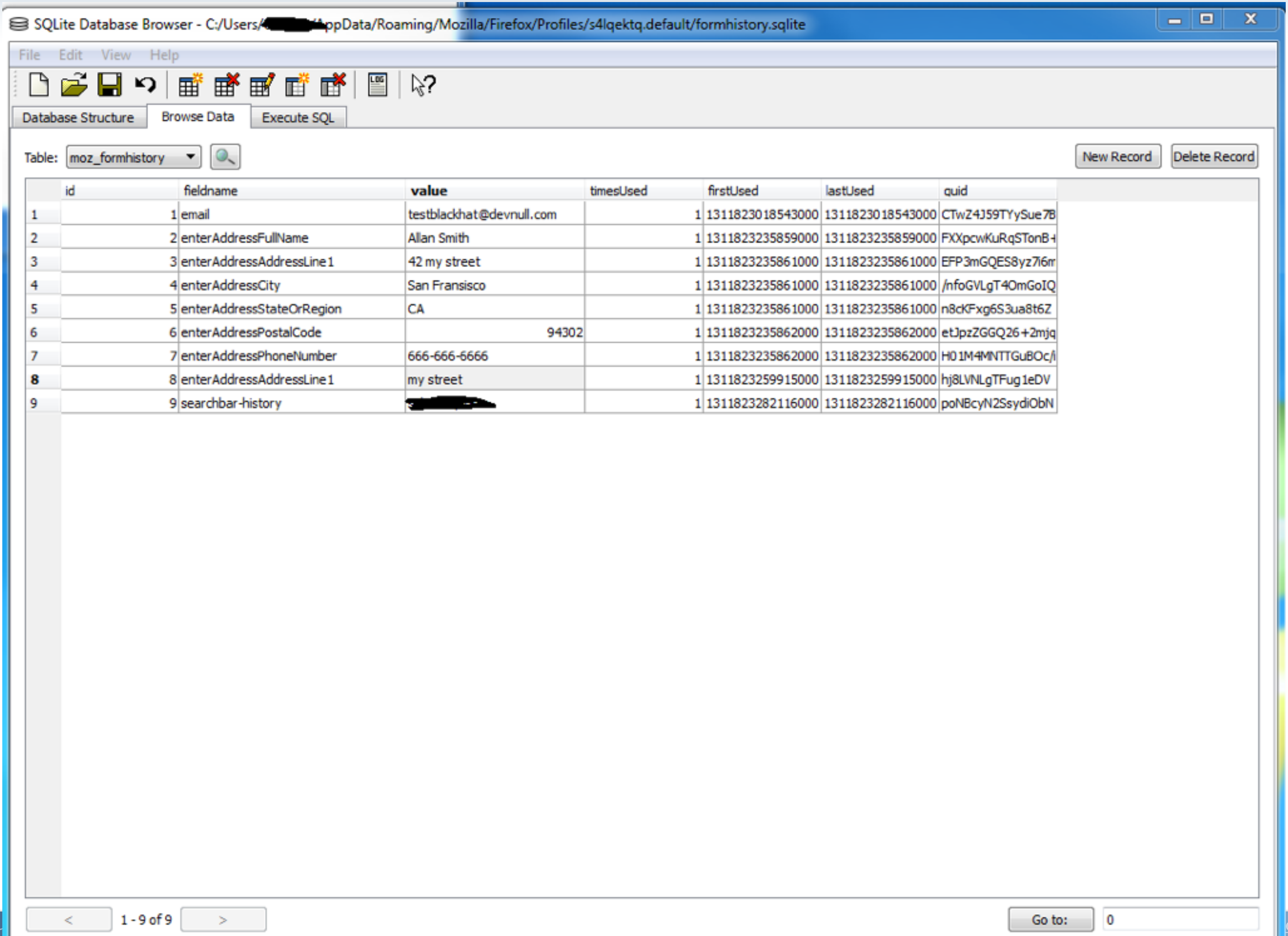
Estimated delivery: Aug. 2, 2011

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

Every form field is recorded

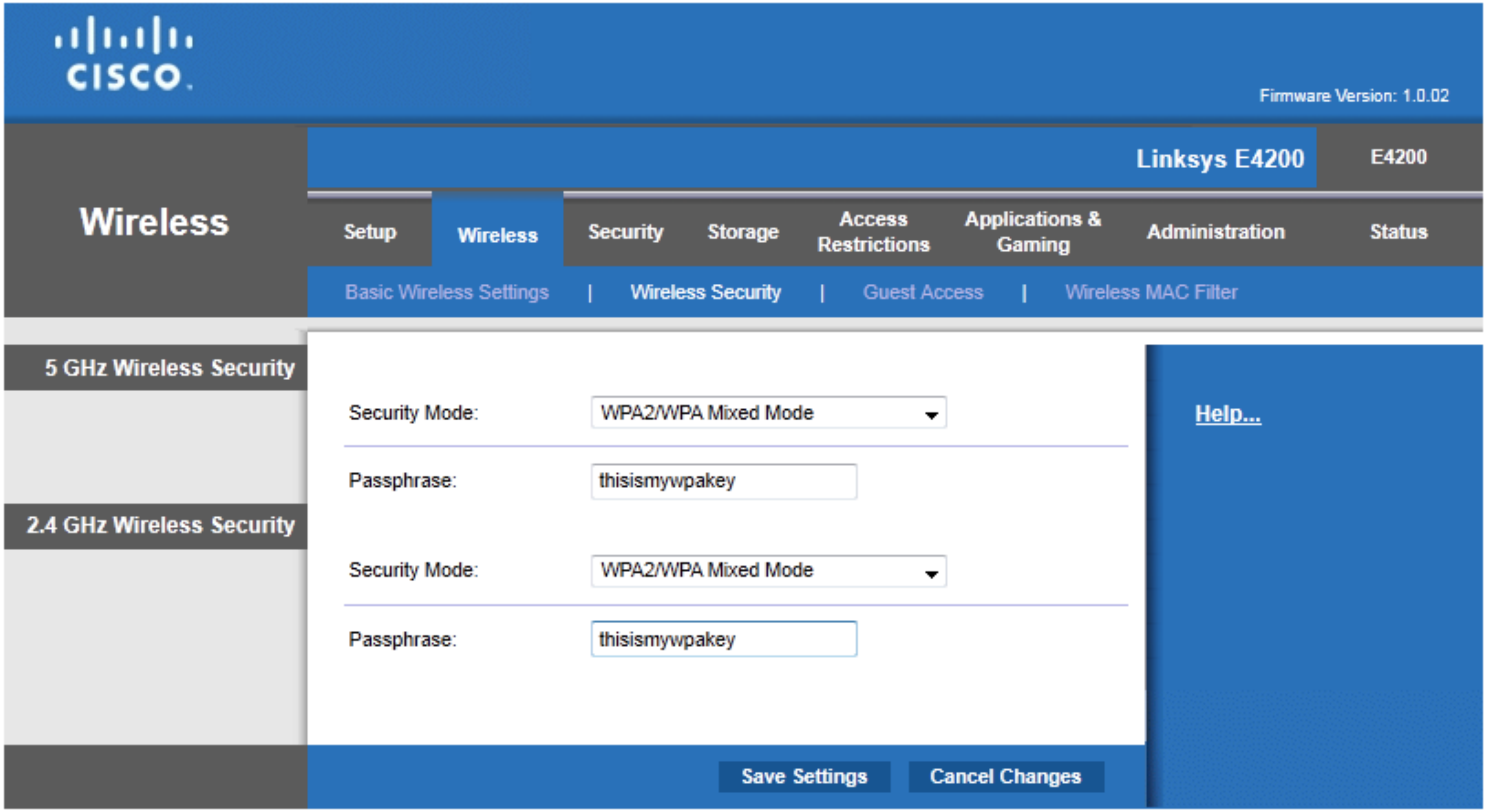


SQLite Database Browser - C:/Users/[redacted]ppData/Roaming/Mozilla/Firefox/Profiles/s4lqektq.default/formhistory.sqlite

Table: moz_formhistory

	id	fieldname	value	timesUsed	firstUsed	lastUsed	guid
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

Configuring a Linksys ?



5 GHz Wireless Security

Security Mode: WPA2/WPA Mixed Mode

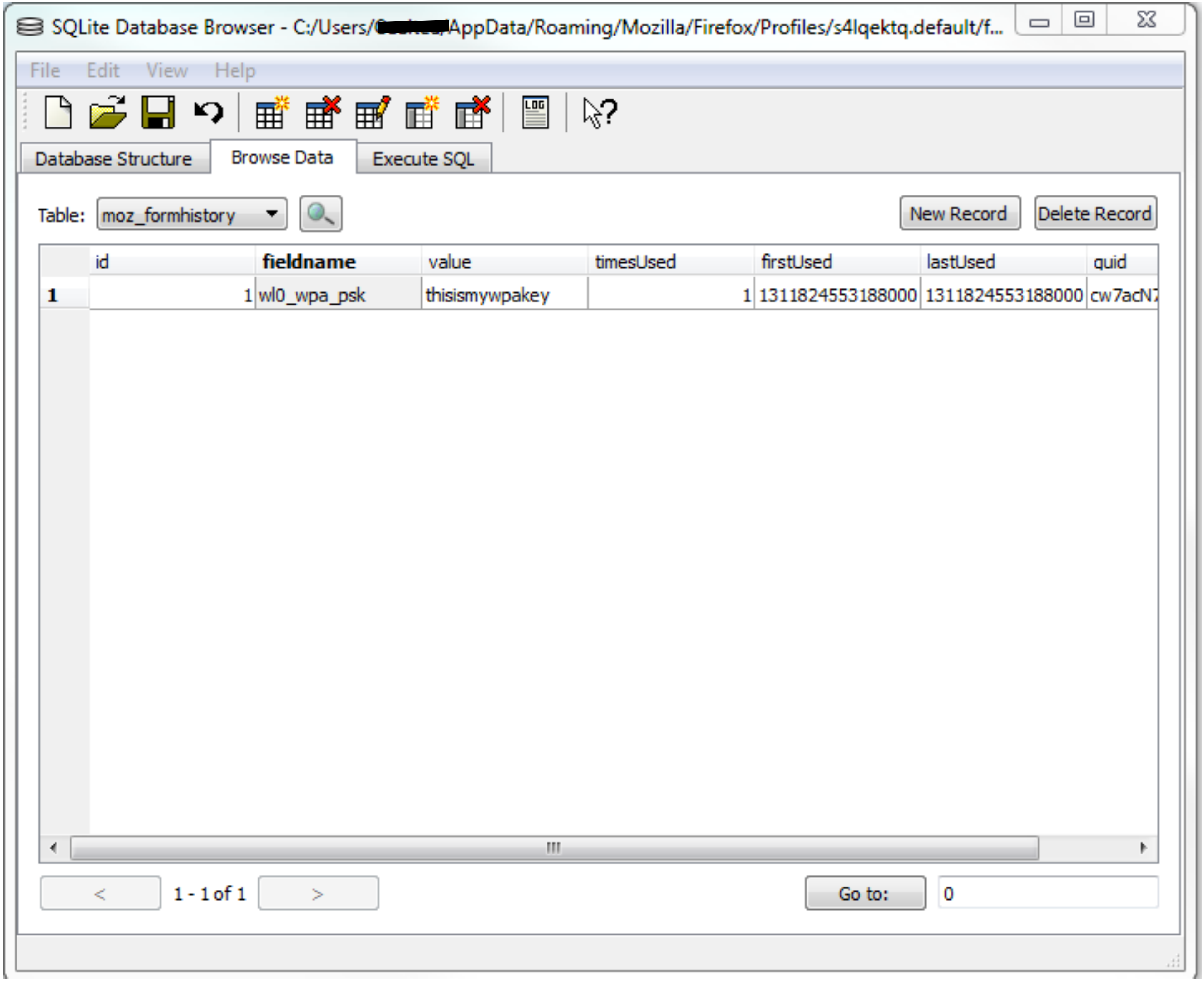
Passphrase: thisismywpakey

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	cw7acN

1 - 1 of 1

0

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

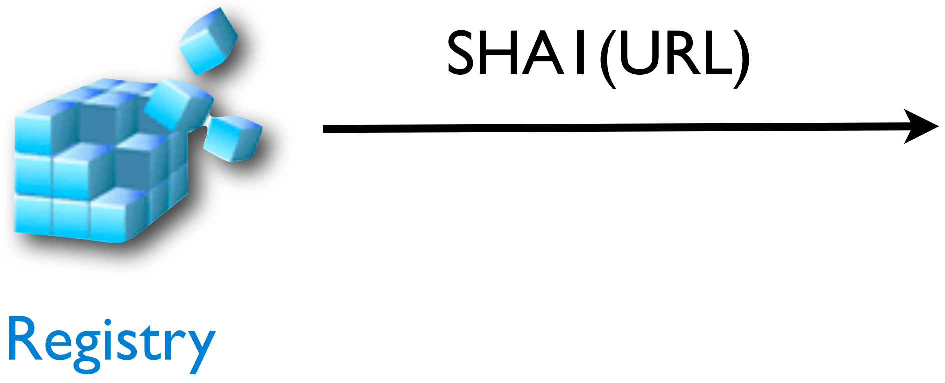
autocomplete=”off”

Internet Explorer

- Passwords
  - Location: registry
  - Encryption: DPAPI + URL as salt
- History
  - URLs: Index.dat

Decrypting Internet Explorer passwords

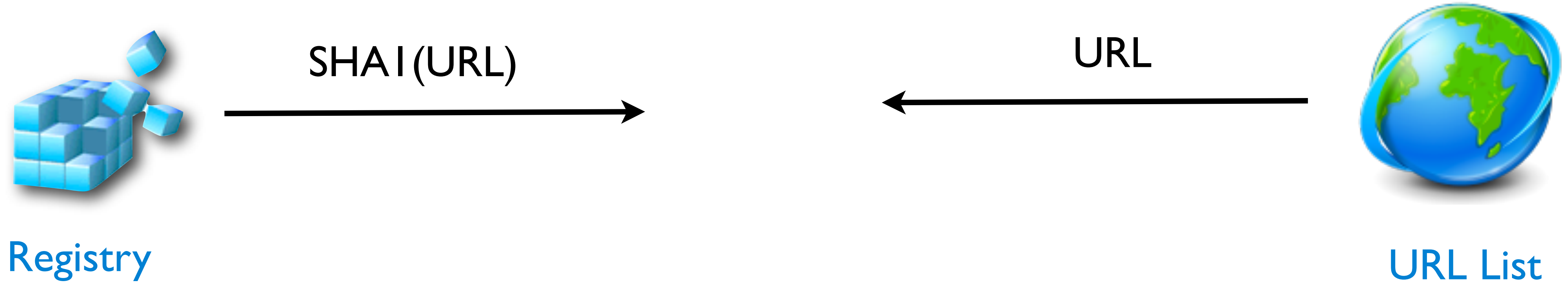
Decrypting Internet Explorer passwords



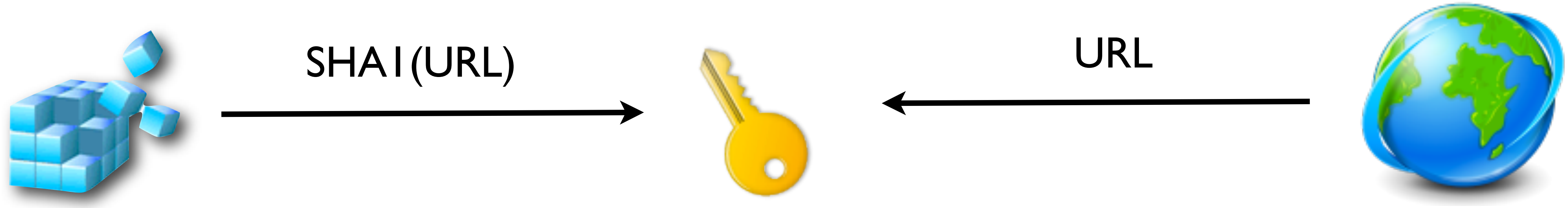
SHA1(URL)

Registry

Decrypting Internet Explorer passwords



Decrypting Internet Explorer passwords



SHA1(URL)

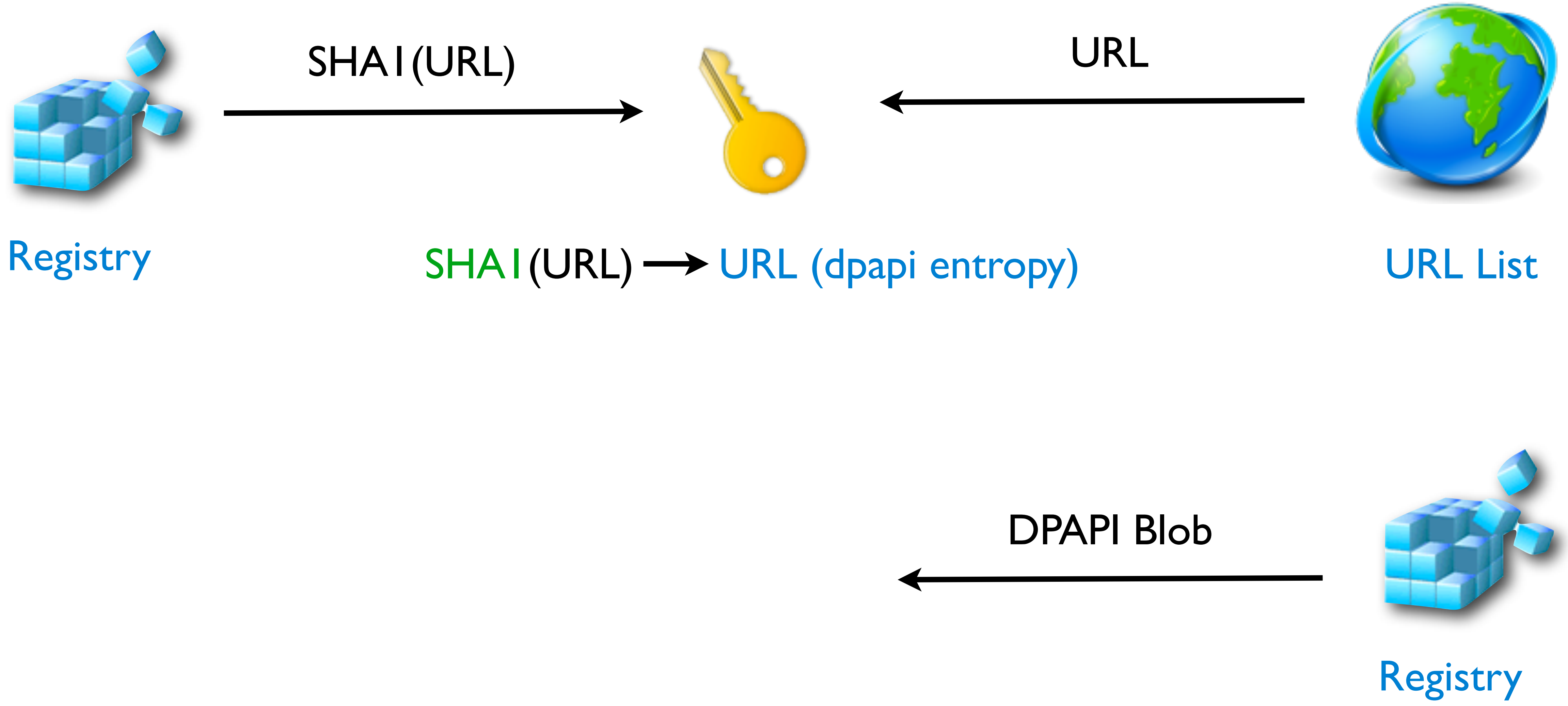
URL

Registry

SHA1(URL) → URL (dpapi entropy)

URL List

Decrypting Internet Explorer passwords



SHA1(URL)

URL

Registry

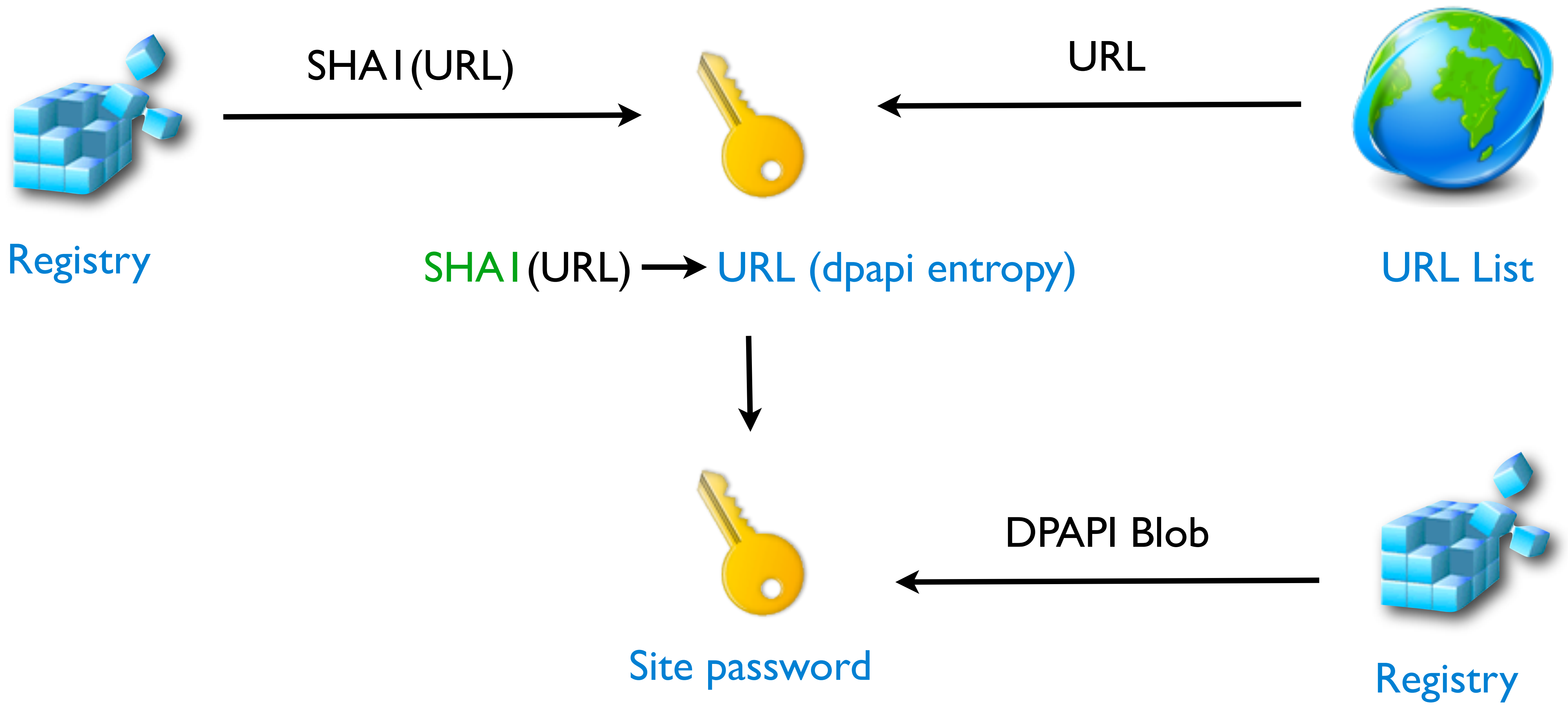
SHA1(URL) → URL (dpapi entropy)

URL List

DPAPI Blob

Registry

Decrypting Internet Explorer passwords



SHA1(URL)

URL

Registry

SHA1(URL) → URL (dpapi entropy)

URL List

DPAPI Blob

Site password

Registry

Maximizing our recovery

- Build a list of URL from others browsers and files
- Use a list of known login URLs

Chrome

- Passwords
  - Location: Login Data (sqlite)
  - Encryption: DPAPI
- History
  - URLs: History (sqlite)
  - Forms fields: Web Data (sqlite)

Safari

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

Browsers takeaway

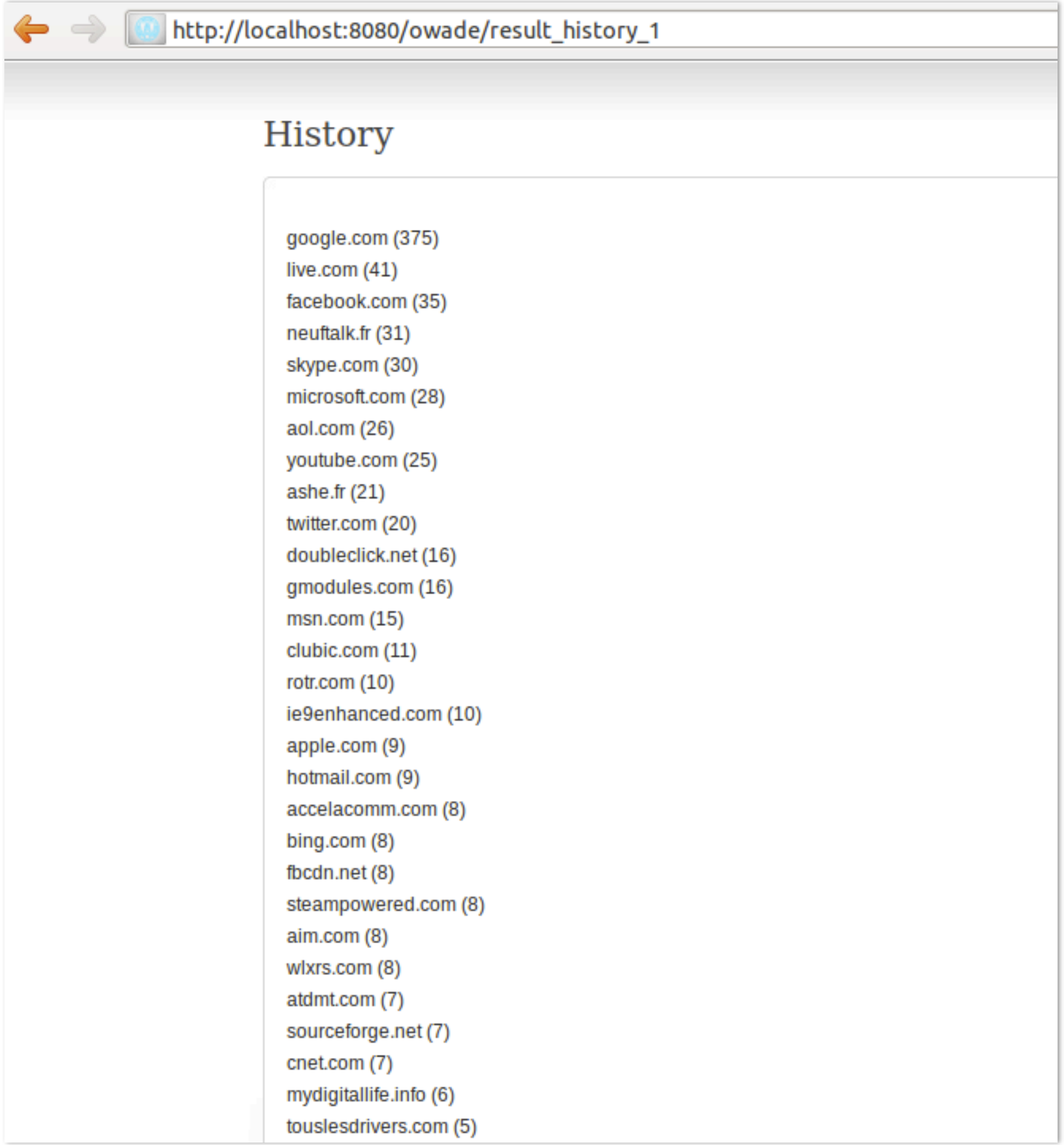
- Internet Explorer is the most secure.
  - If you don’t know the URL you can’t recover the credentials
- Firefox is the worst
  - Passwords encryption not tied to the Windows user password (bug open for a while)
  - Login are encrypted in signons.sqlite not in formhistory.sqlite

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

The browsers histories aggregated



http://localhost:8080/owade/result_history_1

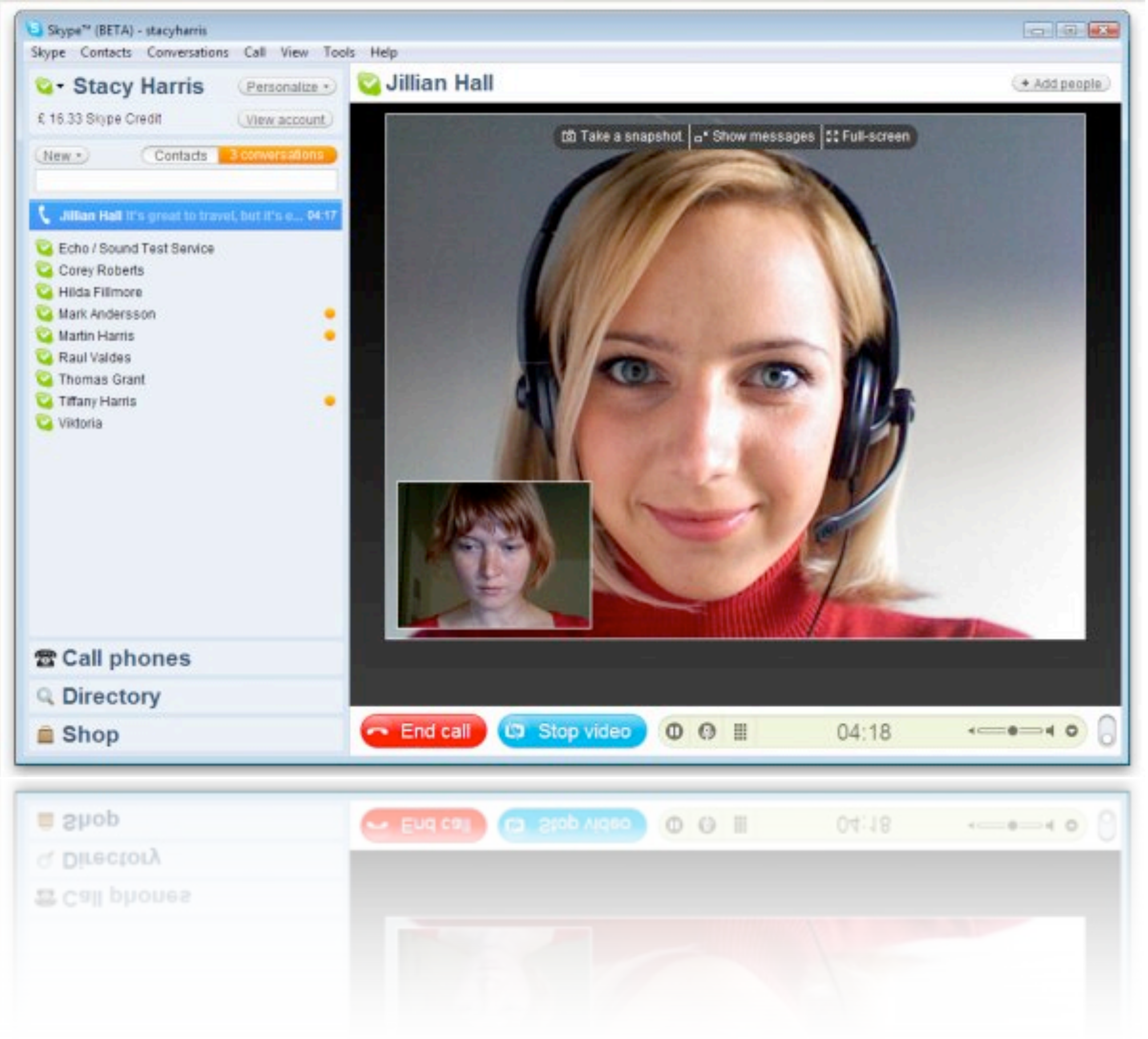
History

google.com (375)
live.com (41)
facebook.com (35)
neuftalk.fr (31)
skype.com (30)
microsoft.com (28)
aol.com (26)
youtube.com (25)
ashe.fr (21)
twitter.com (20)
doubleclick.net (16)
gmodules.com (16)
msn.com (15)
clubic.com (11)
rotr.com (10)
ie9enhanced.com (10)
apple.com (9)
hotmail.com (9)
accelacomm.com (8)
bing.com (8)
fbcdn.net (8)
steampowered.com (8)
aim.com (8)
wlxrs.com (8)
atdmt.com (7)
sourceforge.net (7)
cnet.com (7)
mydigitallife.info (6)
touslesdrivers.com (5)

Instant messaging

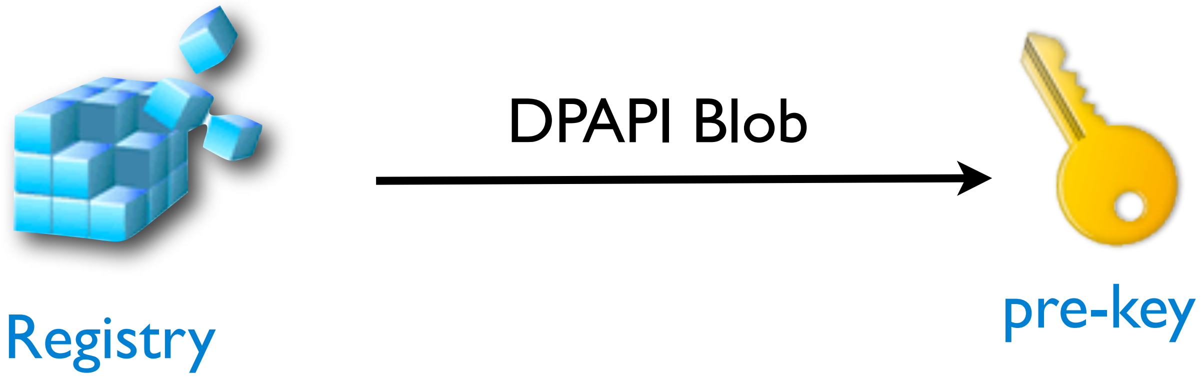
Skype

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



Decrypting Skype passwords

Decrypting Skype passwords

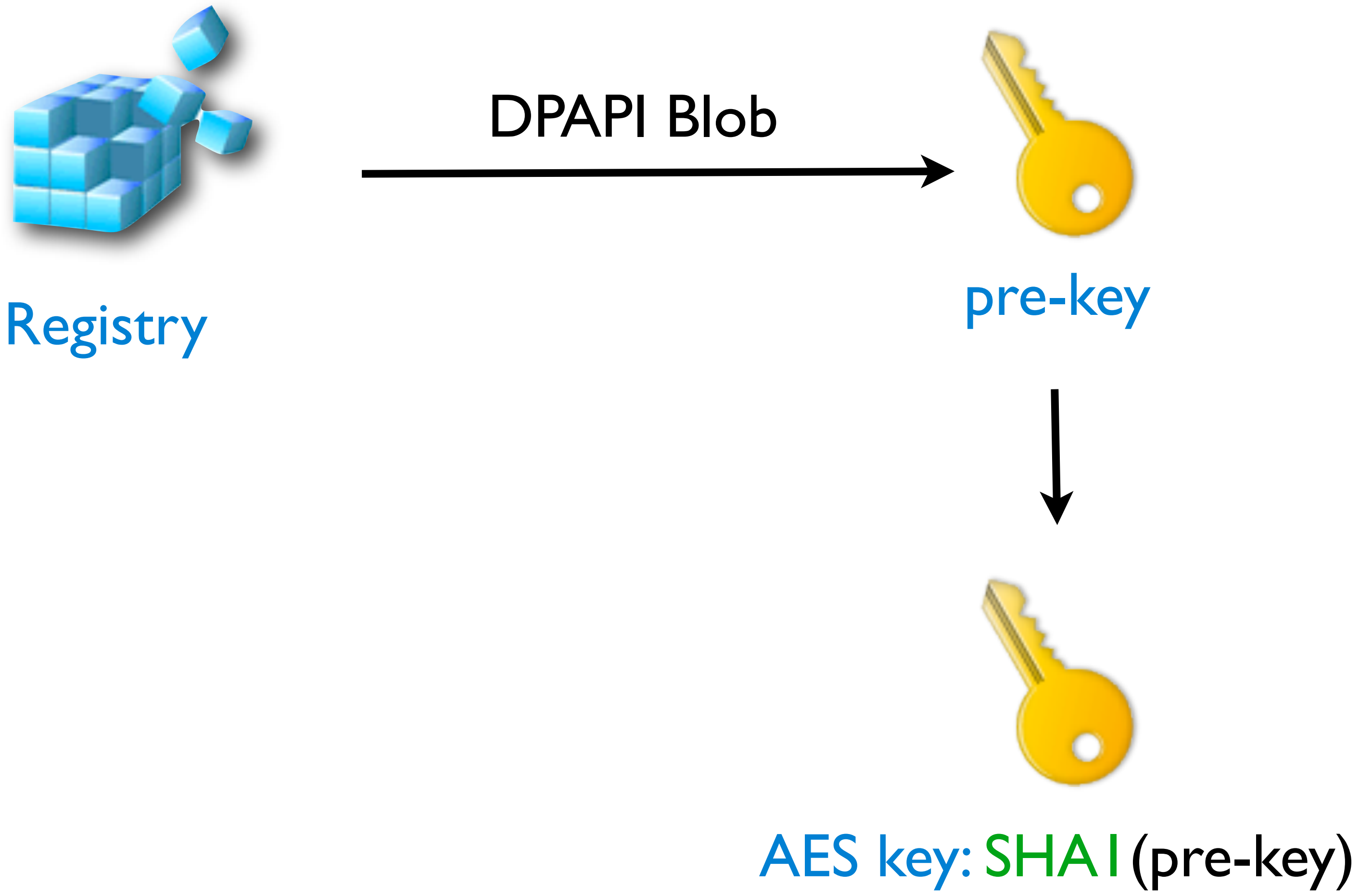


Registry

DPAPI Blob

pre-key

Decrypting Skype passwords



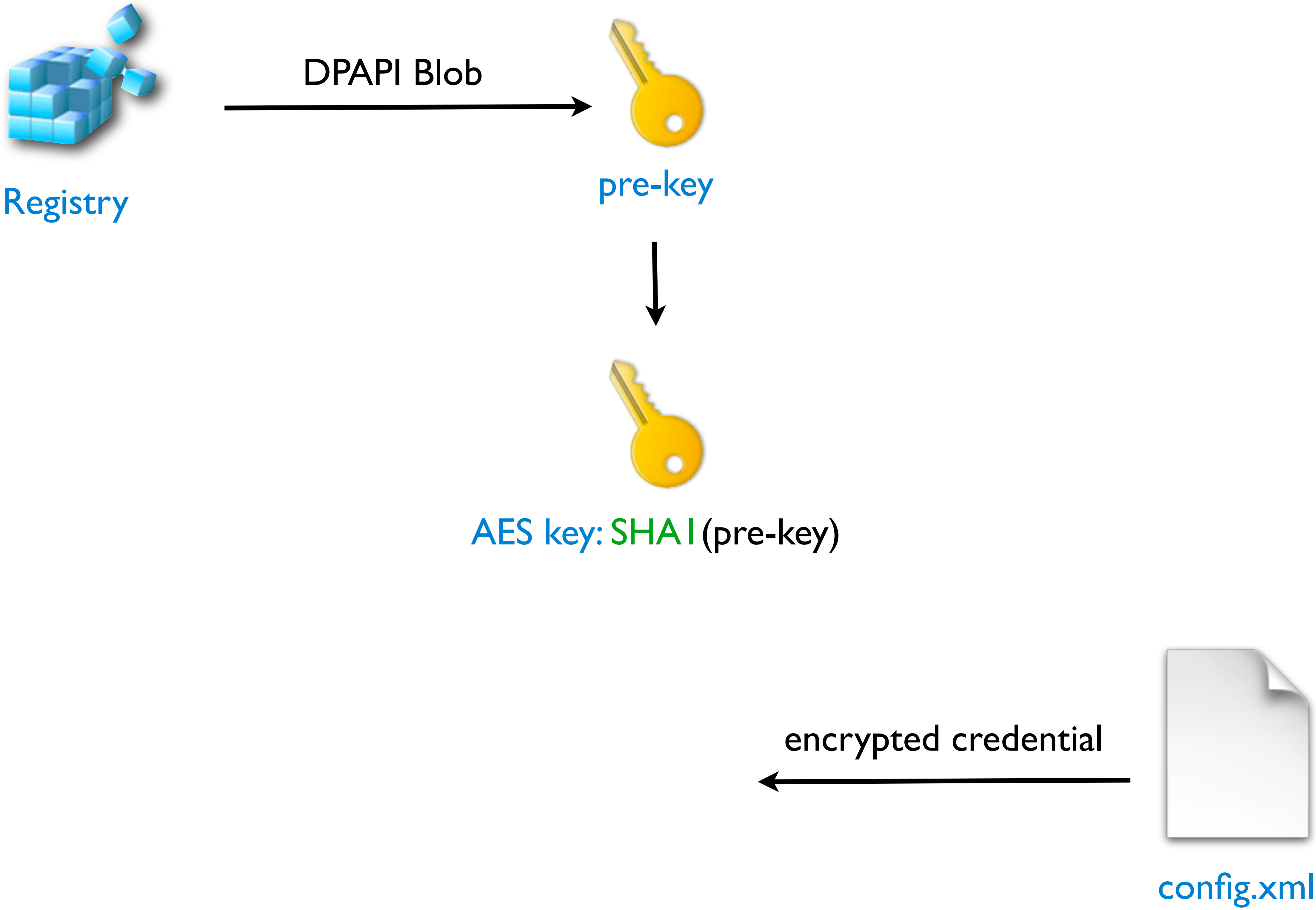
Registry

DPAPI Blob

pre-key

AES key: SHA1(pre-key)

Decrypting Skype passwords



Registry

DPAPI Blob

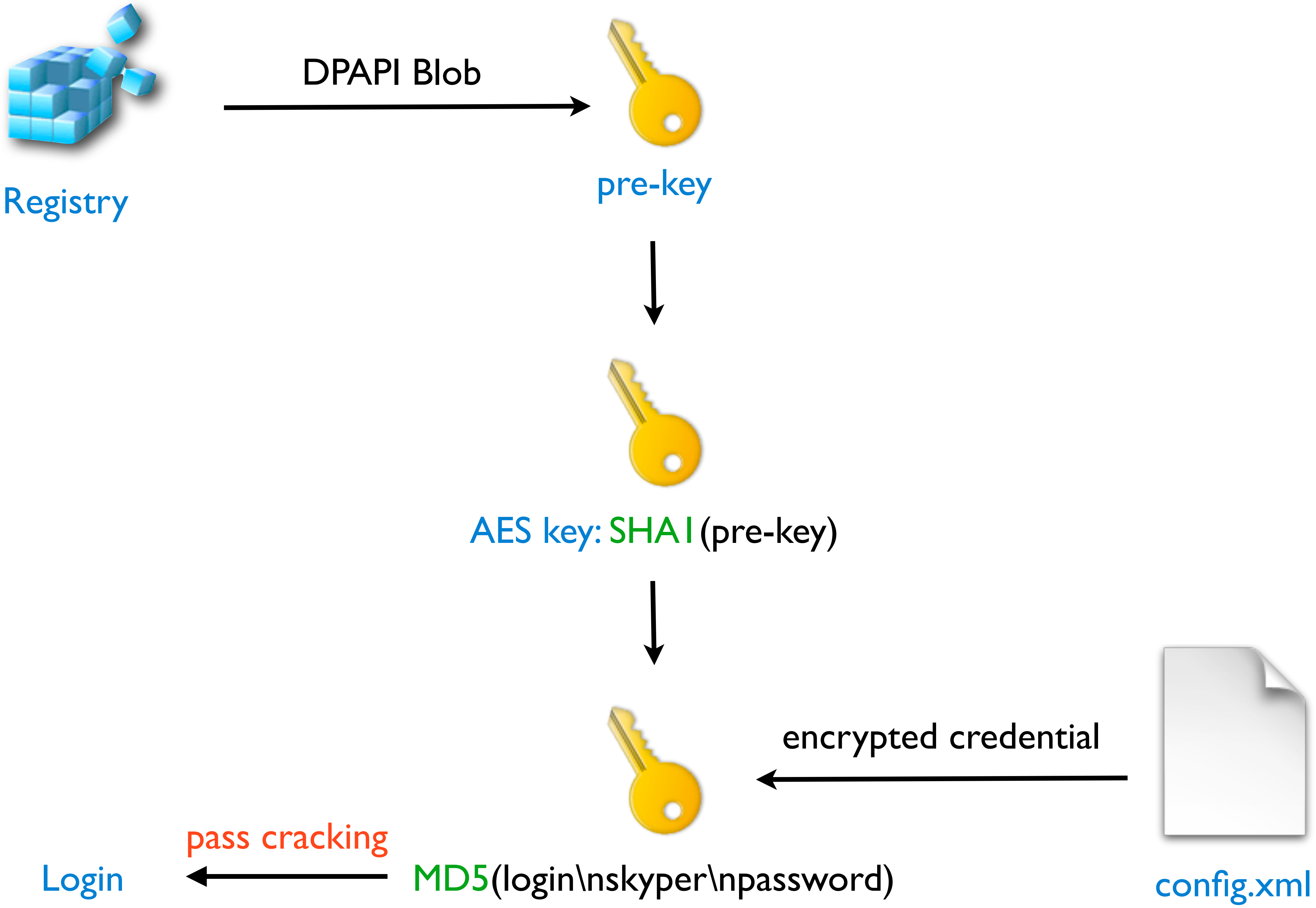
pre-key

AES key: SHA1(pre-key)

encrypted credential

config.xml

Decrypting Skype passwords



Registry

DPAPI Blob

pre-key

AES key: SHA1(pre-key)

encrypted credential

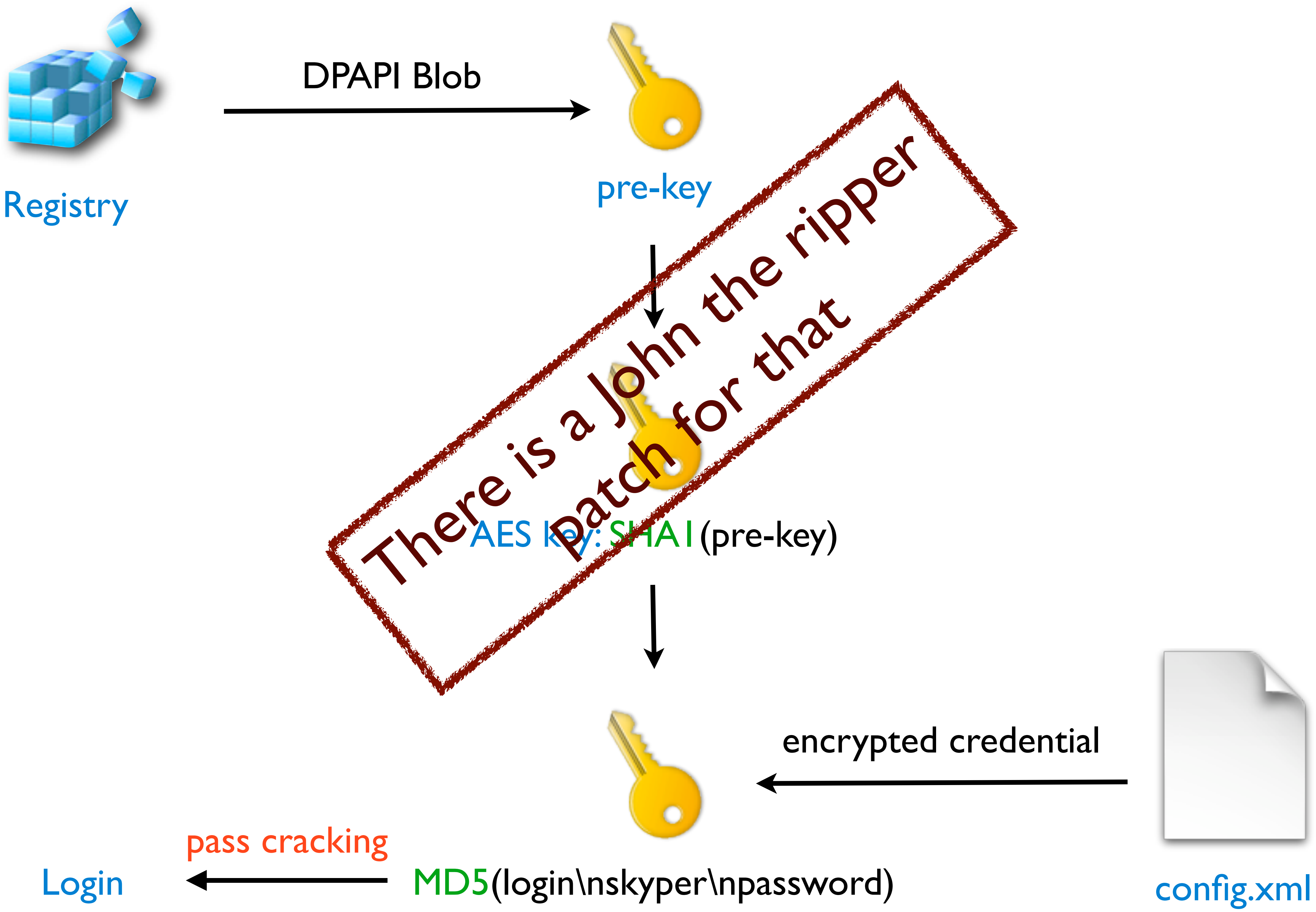
config.xml

MD5(login\nskyper\npassword)

pass cracking

Login

Decrypting Skype passwords



Registry

DPAPI Blob

pre-key

AES key: SHA1(pre-key)

encrypted credential

config.xml

MD5(login\nskyper\npassword)

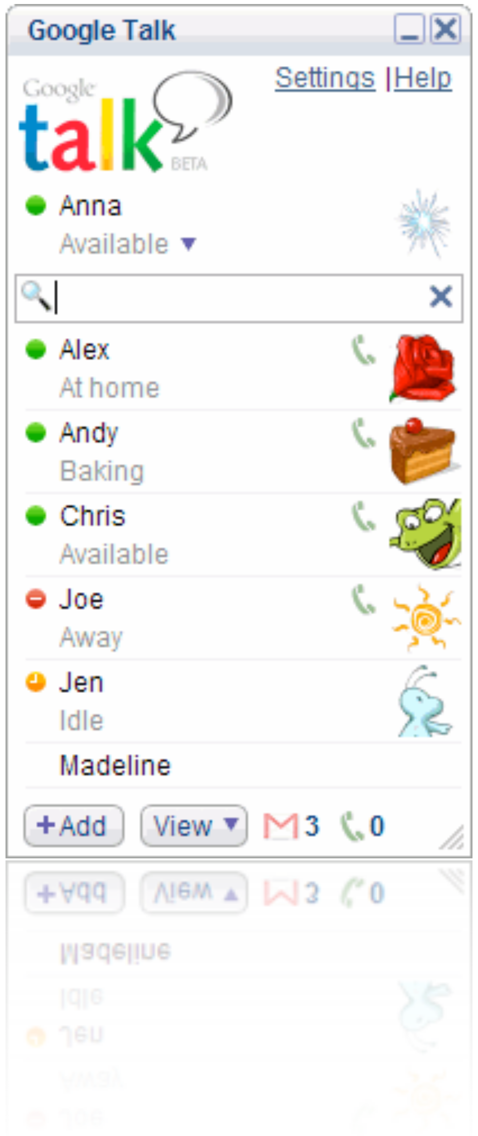
pass cracking

Login

There is a John the ripper patch for that

Google Talk

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



Google Talk

Settings | Help

Anna
Available

Alex
At home

Andy
Baking

Chris
Available

Joe
Away

Jen
Idle

Madeline

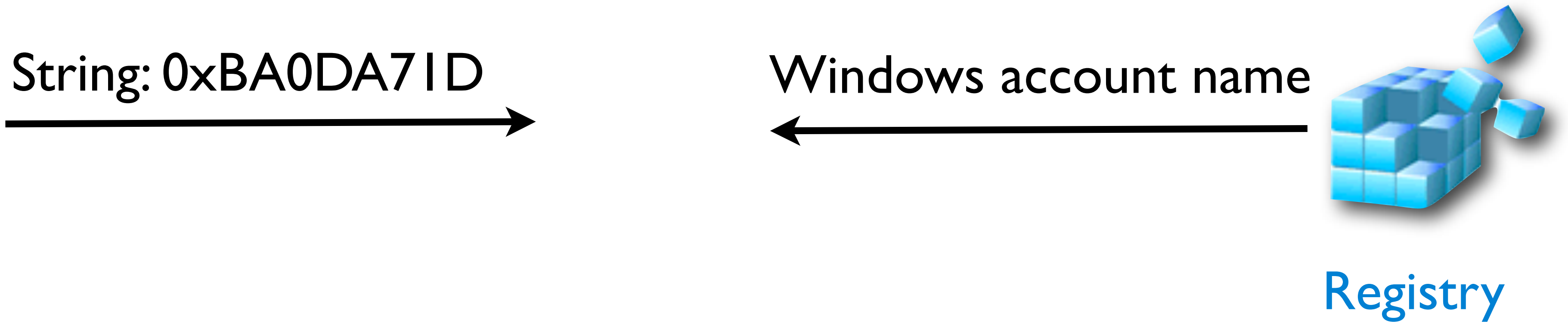
+Add View 3 0

Salt derivation algorithm overview

Salt derivation algorithm overview

String: 0xBA0DA71D

Salt derivation algorithm overview

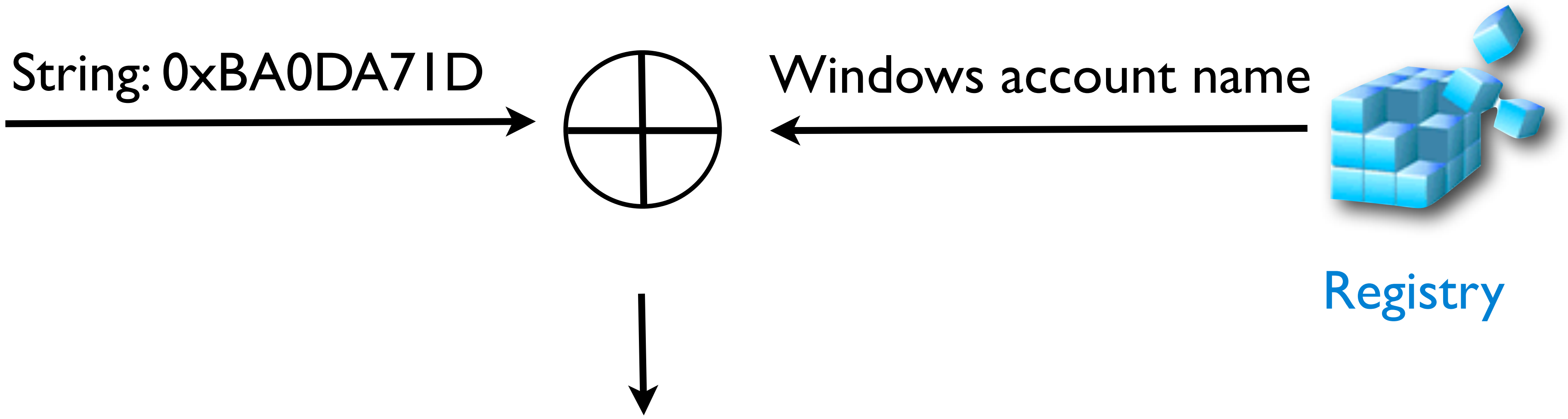


String: 0xBA0DA71D

Windows account name

Registry

Salt derivation algorithm overview

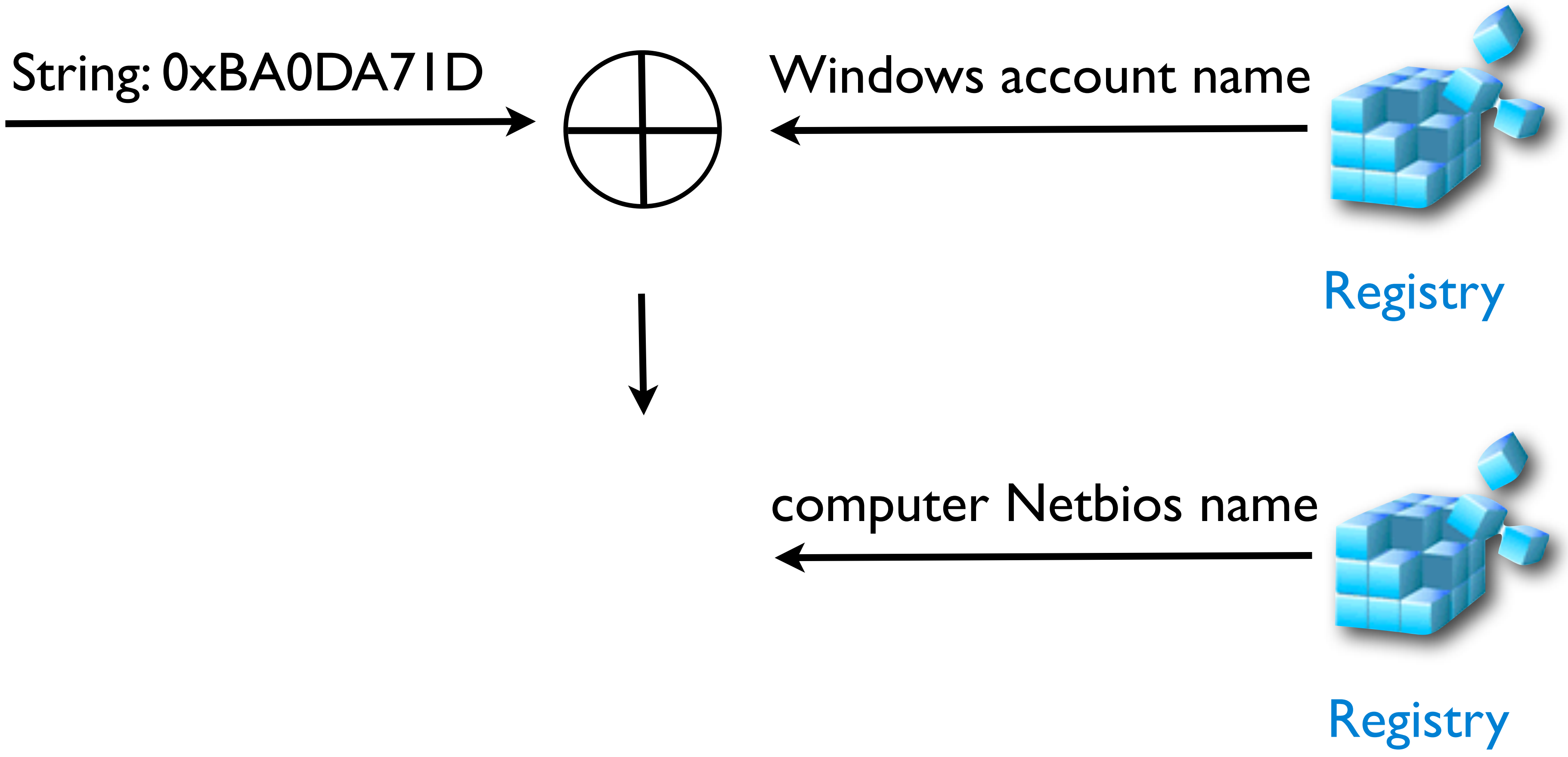


String: 0xBA0DA71D

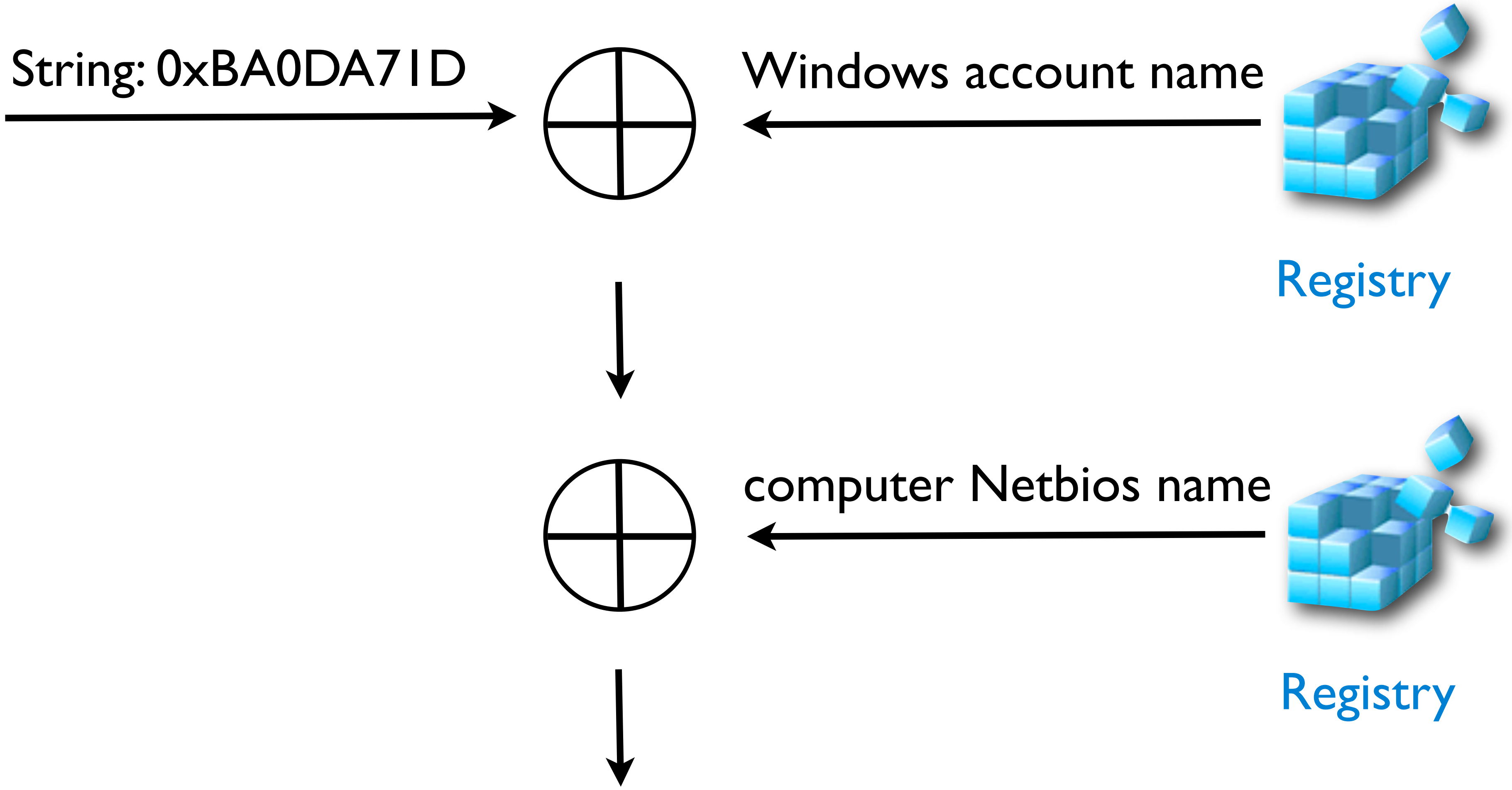
Windows account name

Registry

Salt derivation algorithm overview



Salt derivation algorithm overview



String: 0xBA0DA71D

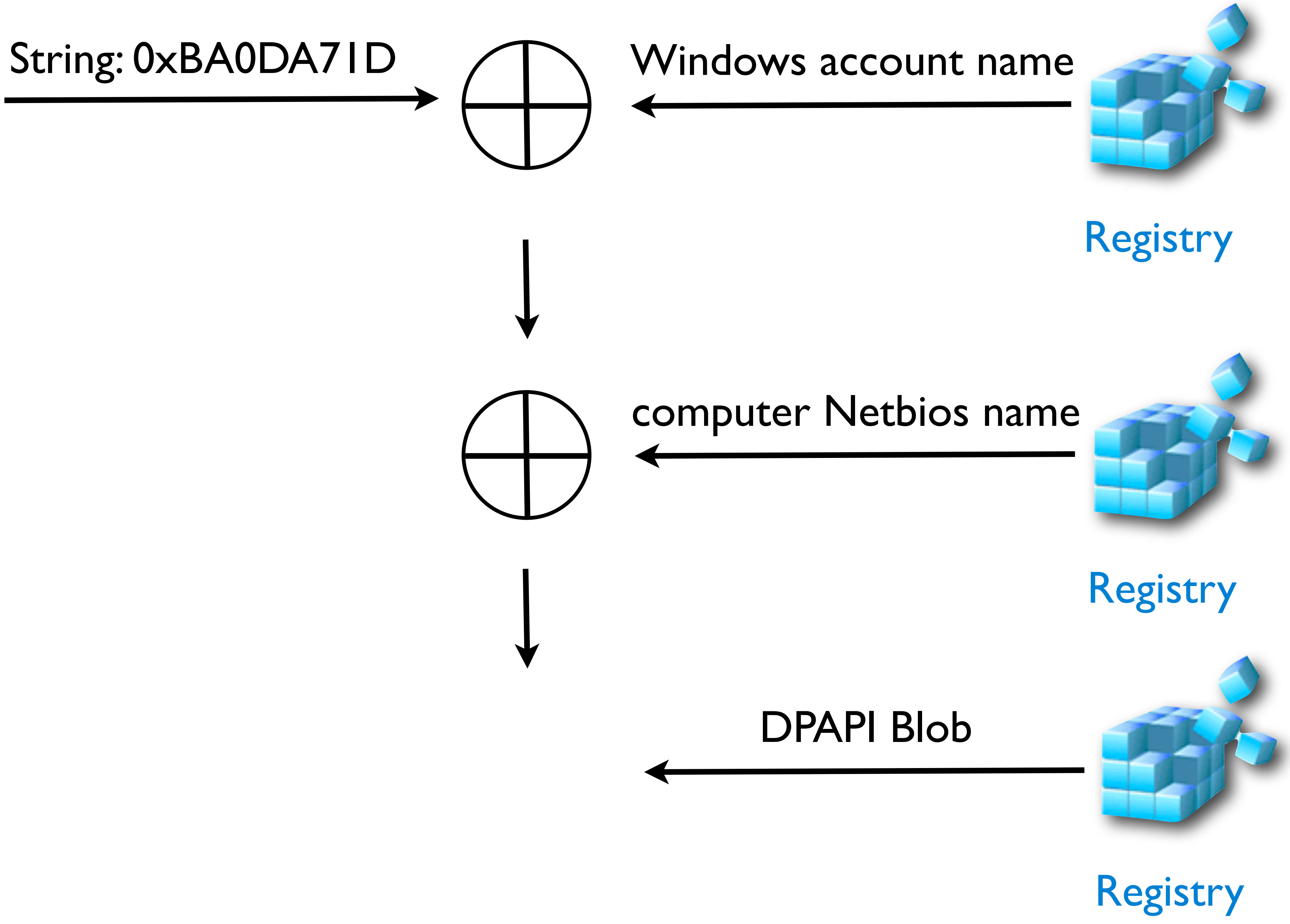
Windows account name

Registry

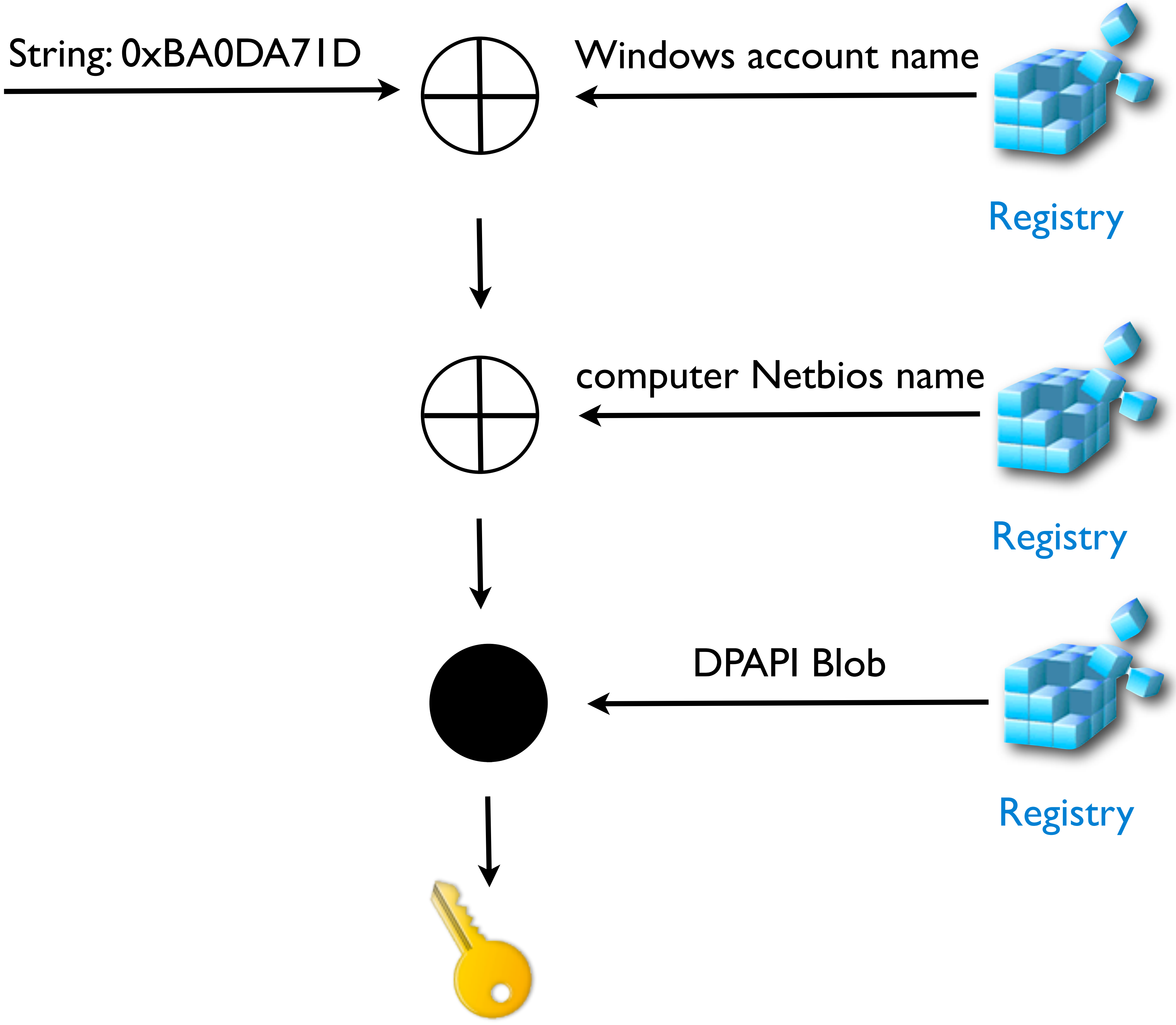
computer Netbios name

Registry

Salt derivation algorithm overview



Salt derivation algorithm overview



String: 0xBA0DA71D

Windows account name

Registry

computer Netbios name

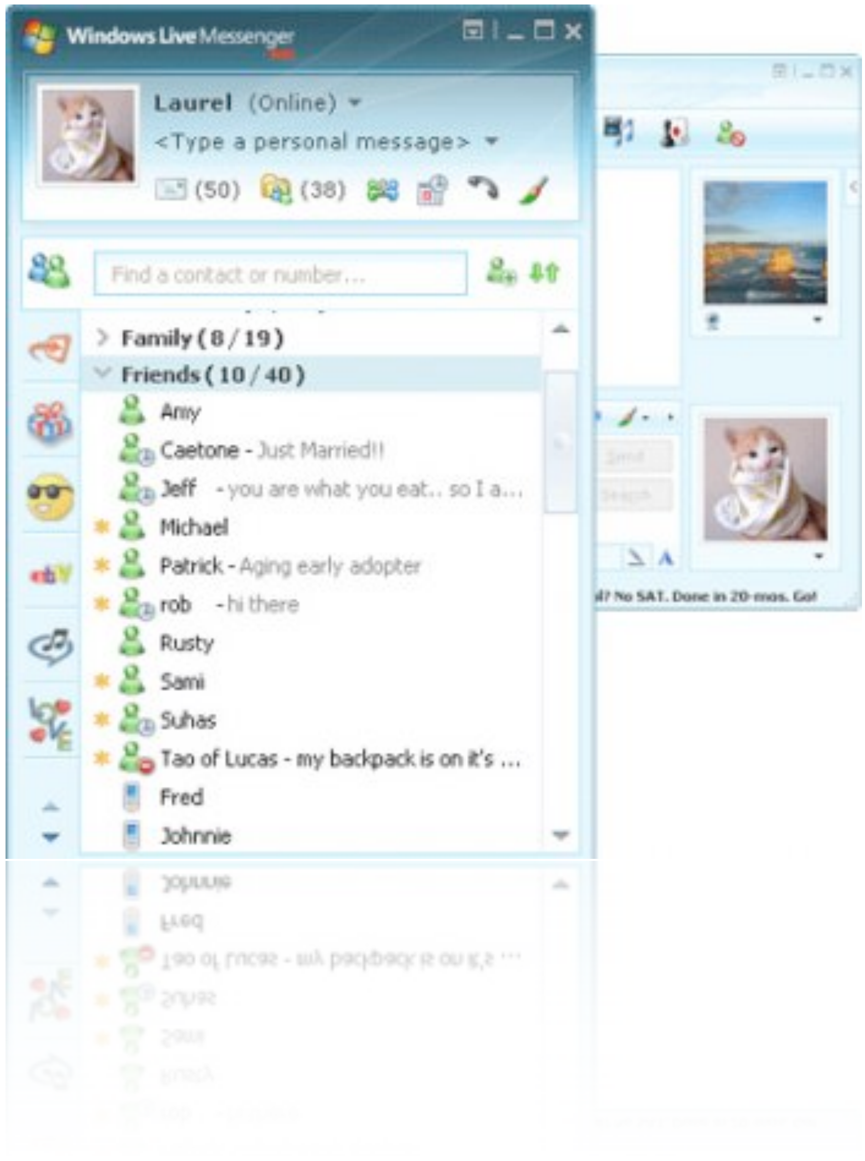
Registry

DPAPI Blob

Registry

Microsoft Messenger

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



Laurel (Online)
<Type a personal message>

Find a contact or number...
Family (8 / 19)
Friends (10 / 40)
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

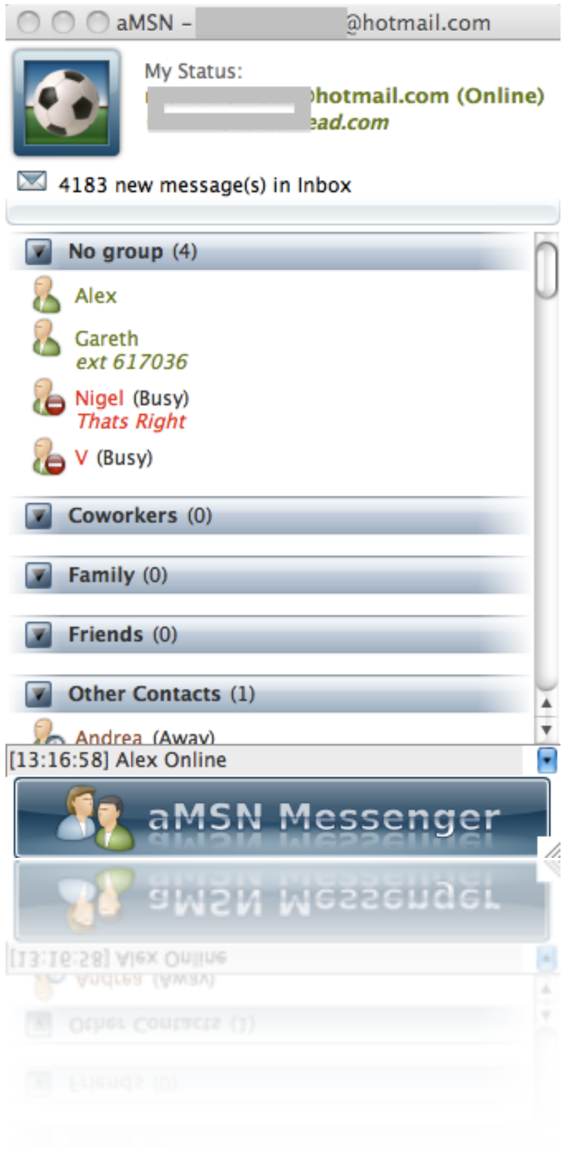
...? No SAT. Done in 20-mos. Go!

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

No group (4)
Alex
Gareth
ext 617036
Nigel (Busy)
Thats Right
V (Busy)
Coworkers (0)
Family (0)
Friends (0)
Other Contacts (1)
Andrea (Away)

[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

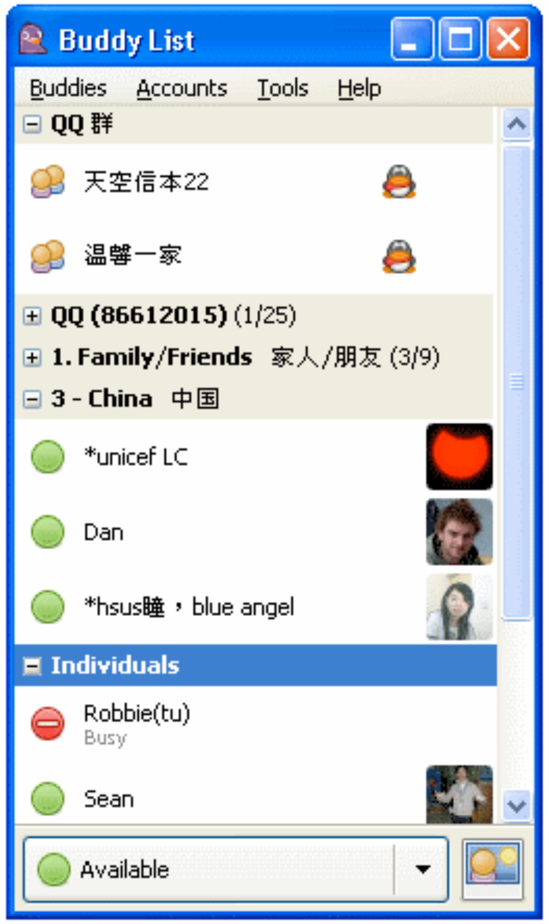
  trivial

- Location

  user.config

Pidgin

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



QQ 群

天空信本22

温馨一家

QQ (86612015) (1/25)

1. Family/Friends 家人/朋友 (3/9)

3 - China 中国

*unicef LC

Dan

*hsus睫，blue angel

Individuals

Robbie(tu)
Busy

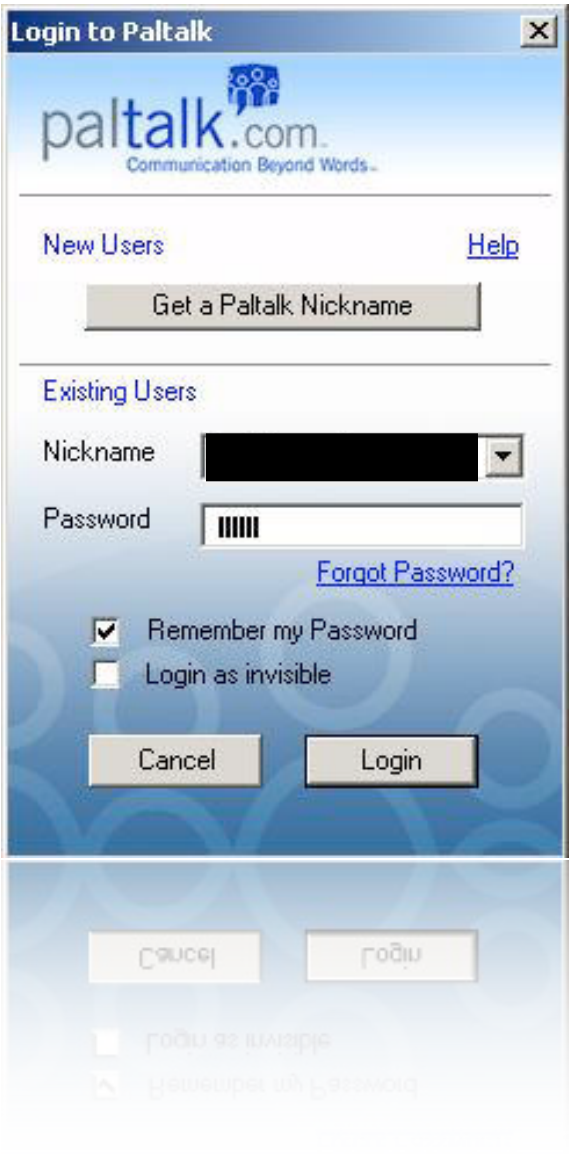
Sean

Pidgin

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

Paltalk

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



Login to Paltalk ☒

New Users Help

Existing Users

Nickname [redacted]

Password IIIIII

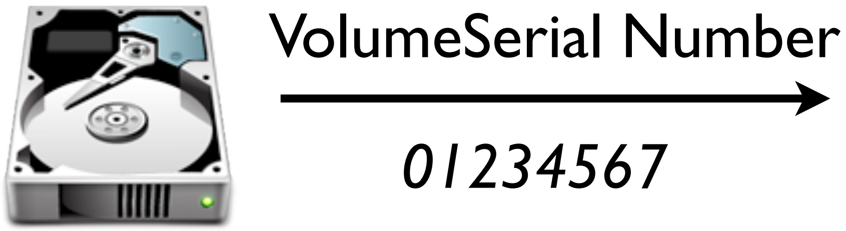
Forgot Password?

☑ Remember my Password

□ Login as invisible

Paltalk encryption algorithm

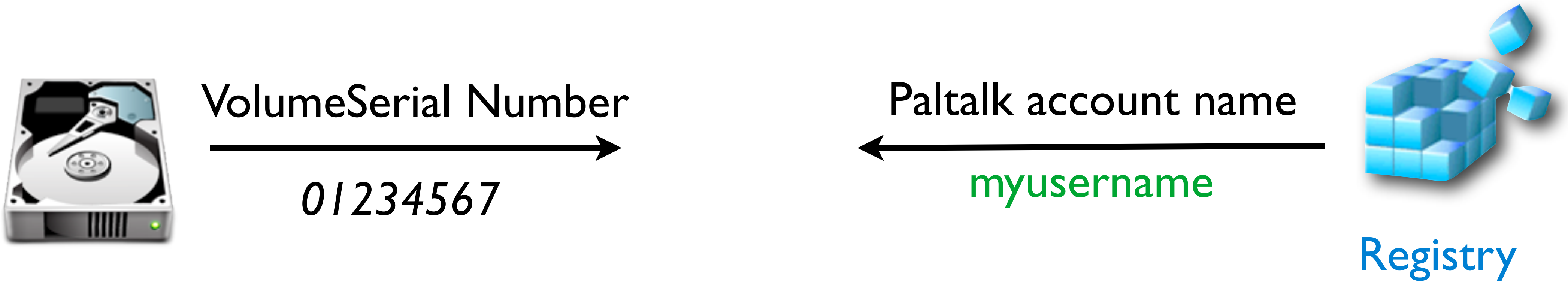
Paltalk encryption algorithm



VolumeSerial Number

01234567

Paltalk encryption algorithm



VolumeSerial Number

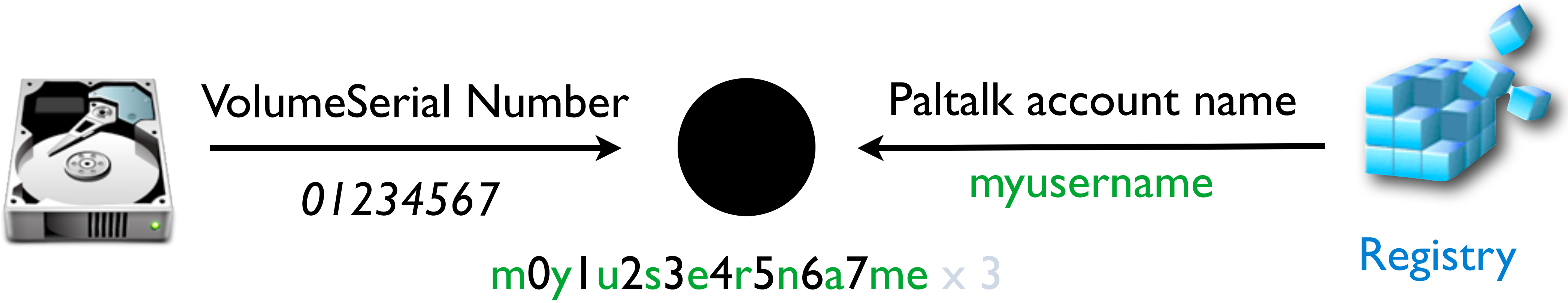
01234567

Paltalk account name

myusername

Registry

Paltalk encryption algorithm



VolumeSerial Number

01234567

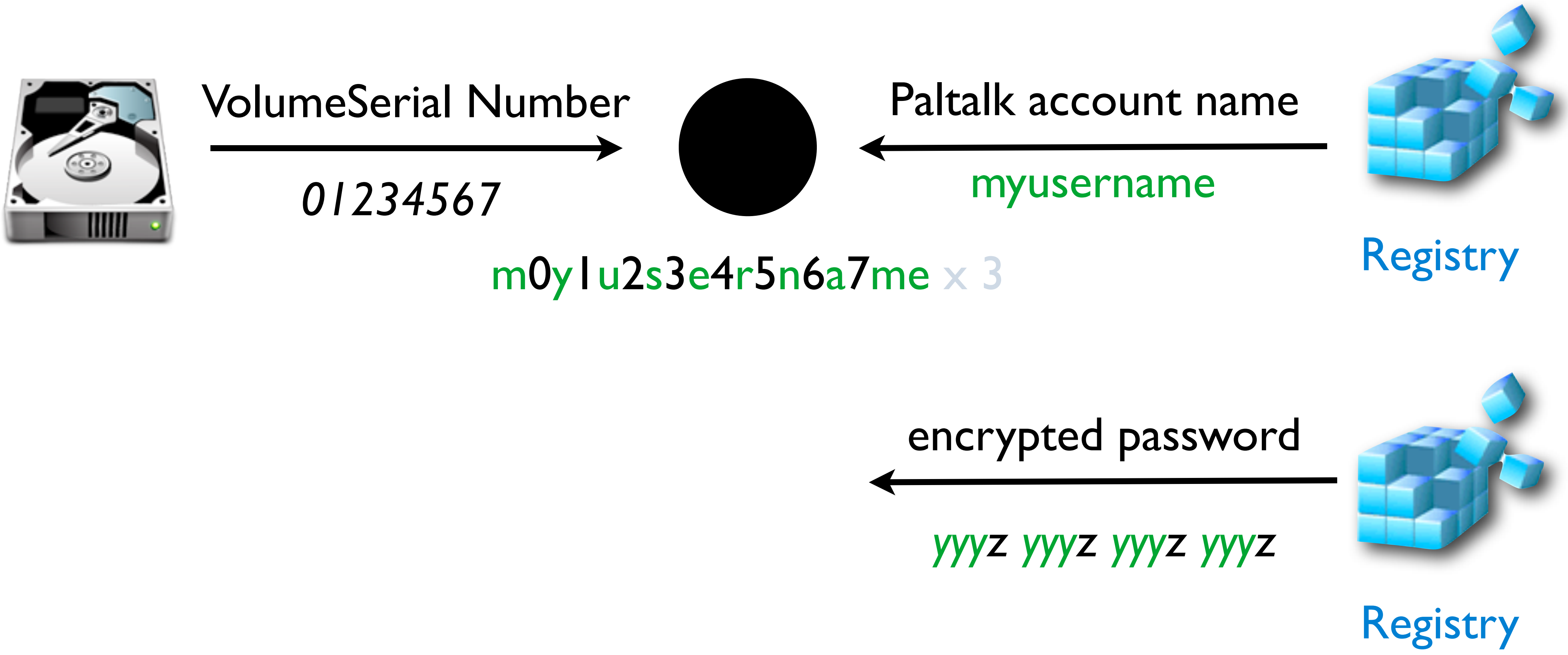
Paltalk account name

myusername

Registry

m0y1u2s3e4r5n6a7me x 3

Paltalk encryption algorithm



VolumeSerial Number

01234567

Paltalk account name

myusername

Registry

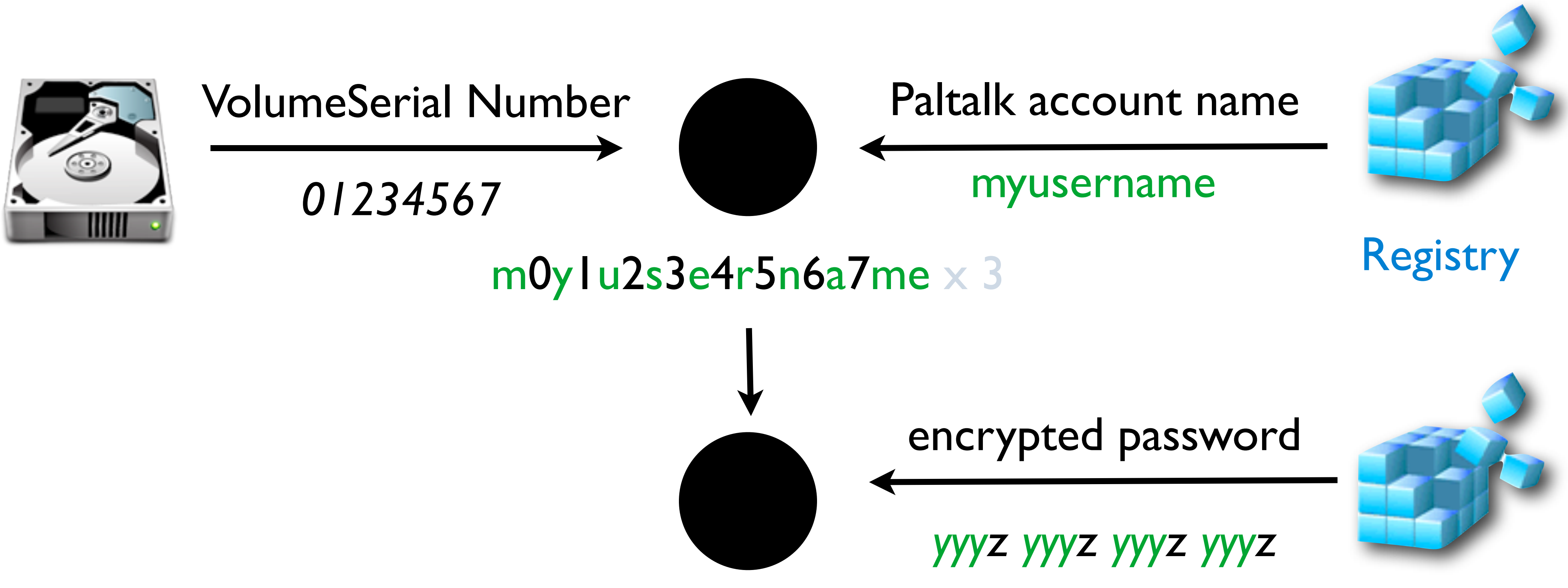
m0y1u2s3e4r5n6a7me x 3

encrypted password

*yyy*z *yyy*z *yyy*z *yyy*z

Registry

Paltalk encryption algorithm



VolumeSerial Number

01234567

Paltalk account name

myusername

Registry

m0y1u2s3e4r5n6a7me x 3

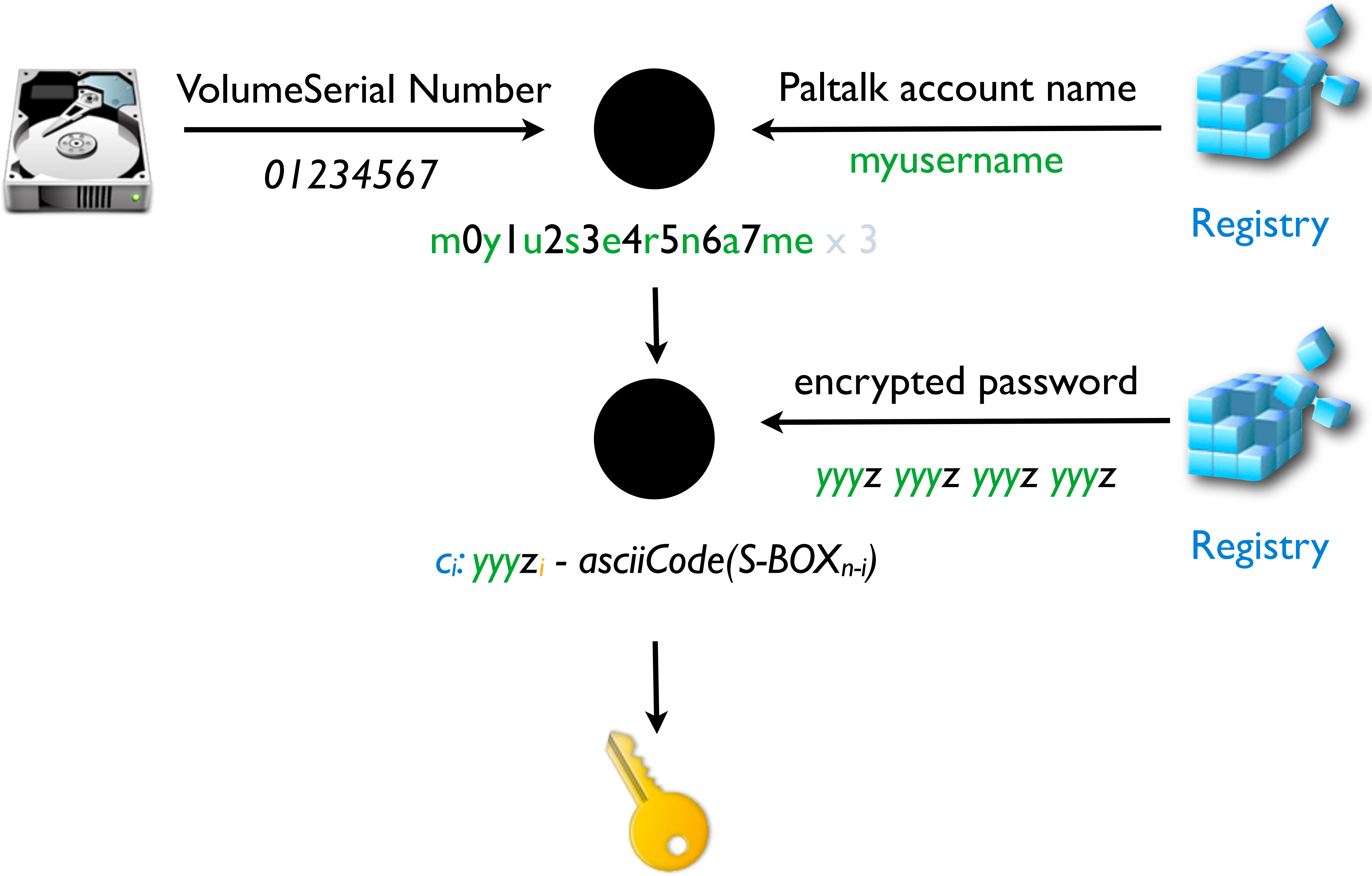
encrypted password

*yyy*z *yyy*z *yyy*z *yyy*z

Registry

c_i: *yyy*z$_i$ - *asciiCode(S-BOX$_{n-i}$)*

Paltalk encryption algorithm



VolumeSerial Number

01234567

Paltalk account name

myusername

Registry

m0y1u2s3e4r5n6a7me x 3

encrypted password

*yyy*z *yyy*z *yyy*z *yyy*z

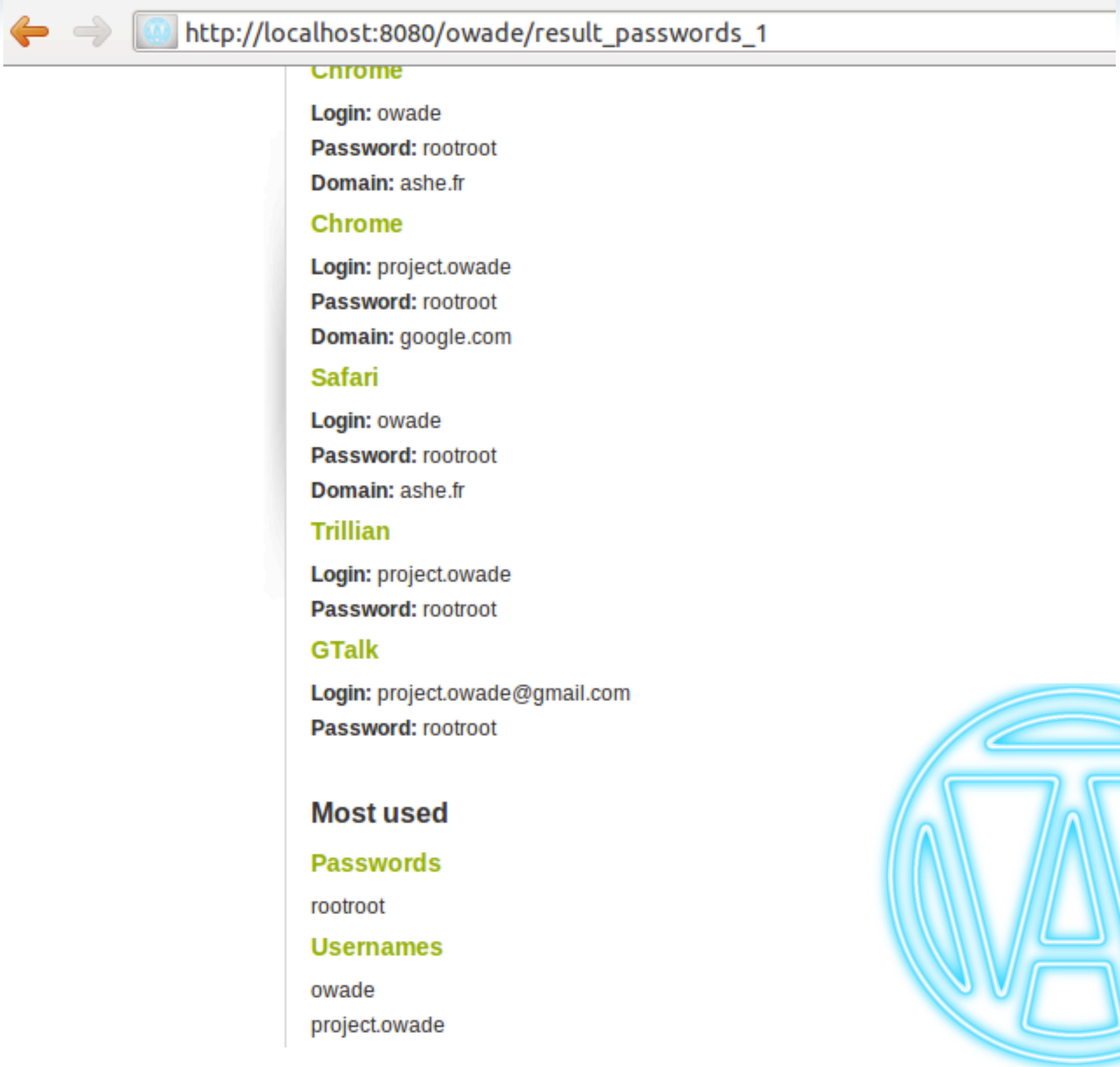
Registry

c_i: *yyy*z$_i$ - *asciiCode(S-BOX$_{n-i}$)*

Messenger take away

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

All the credentials recovered by OWADE



http://localhost:8080/owade/result_passwords_1

Chrome

Login: owade

Password: rootroot

Domain: ashe.fr

Chrome

Login: project.owade

Password: rootroot

Domain: google.com

Safari

Login: owade

Password: rootroot

Domain: ashe.fr

Trillian

Login: project.owade

Password: rootroot

GTalk

Login: project.owade@gmail.com

Password: rootroot

Most used

Passwords

rootroot

Usernames

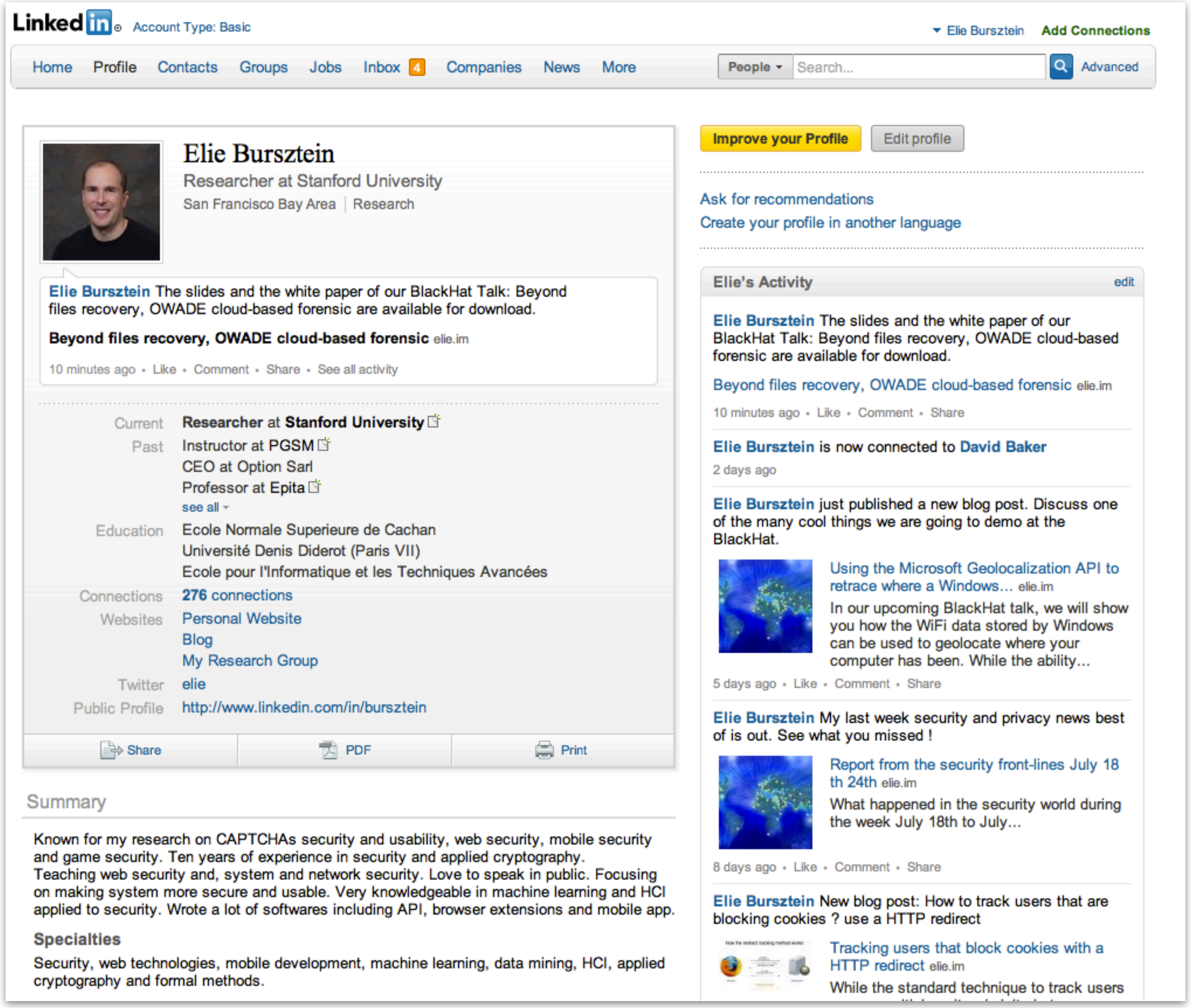
owade

project.owade

Cloud based forensic

Cloud modules

- Leverage the credentials and history extracted to get cloud-data
- Might be legal (or not)
- Only LinkedIn currently (more modules almost ready)



Elie Bursztein

Researcher at Stanford University

San Francisco Bay Area | Research

Elie Bursztein The slides and the white paper of our BlackHat Talk: Beyond files recovery, OWADE cloud-based forensic are available for download.

Beyond files recovery, OWADE cloud-based forensic elie.im

10 minutes ago • Like • Comment • Share • See all activity

Current	**Researcher** at **Stanford University**
Past	Instructor at PGSM CEO at Option Sarl Professor at Epita see all
Education	Ecole Normale Superieure de Cachan Université Denis Diderot (Paris VII) Ecole pour l'Informatique et les Techniques Avancées
Connections	276 connections
Websites	Personal Website Blog My Research Group
Twitter	elie
Public Profile	http://www.linkedin.com/in/bursztein

Summary

Known for my research on CAPTCHAs security and usability, web security, mobile security and game security. Ten years of experience in security and applied cryptography. Teaching web security and, system and network security. Love to speak in public. Focusing on making system more secure and usable. Very knowledgeable in machine learning and HCI applied to security. Wrote a lot of softwares including API, browser extensions and mobile app.

Specialties

Security, web technologies, mobile development, machine learning, data mining, HCI, applied cryptography and formal methods.

Ask for recommendations

Create your profile in another language

Elie's Activity

Elie Bursztein The slides and the white paper of our BlackHat Talk: Beyond files recovery, OWADE cloud-based forensic are available for download.

Beyond files recovery, OWADE cloud-based forensic elie.im

10 minutes ago • Like • Comment • Share

Elie Bursztein is now connected to David Baker

2 days ago

Elie Bursztein just published a new blog post. Discuss one of the many cool things we are going to demo at the BlackHat.

Using the Microsoft Geolocalization API to retrace where a Windows... elie.im

In our upcoming BlackHat talk, we will show you how the WiFi data stored by Windows can be used to geolocate where your computer has been. While the ability...

5 days ago • Like • Comment • Share

Elie Bursztein My last week security and privacy news best of is out. See what you missed !

Report from the security front-lines July 18 th 24th elie.im

What happened in the security world during the week July 18th to July...

8 days ago • Like • Comment • Share

Elie Bursztein New blog post: How to track users that are blocking cookies ? use a HTTP redirect

Tracking users that block cookies with a HTTP redirect elie.im

While the standard technique to track users

OWADE status

- Alpha stage
  - Tested on Ubuntu against XP windows
- Roadmap
  - Stabilizing the code
  - modularize the code so you write your own modules
  - More cloud probes: Facebook, Flickr, Emails...
  - Windows Vista and 7 integration

Conclusion

- People moving to the cloud means more data that are 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

Thank you !

Download OWADE

http://owade.org

Follow-us on Twitter

@elie, @projectowade

Donate to OWADE to support it !