

Gathering Open Source Intelligence Anonymously

Background

- Founded Anonymizer in 1995
- Creating Solutions Since 1992
- Known for Consumer Privacy Service
- Major Corporate and Government Customers



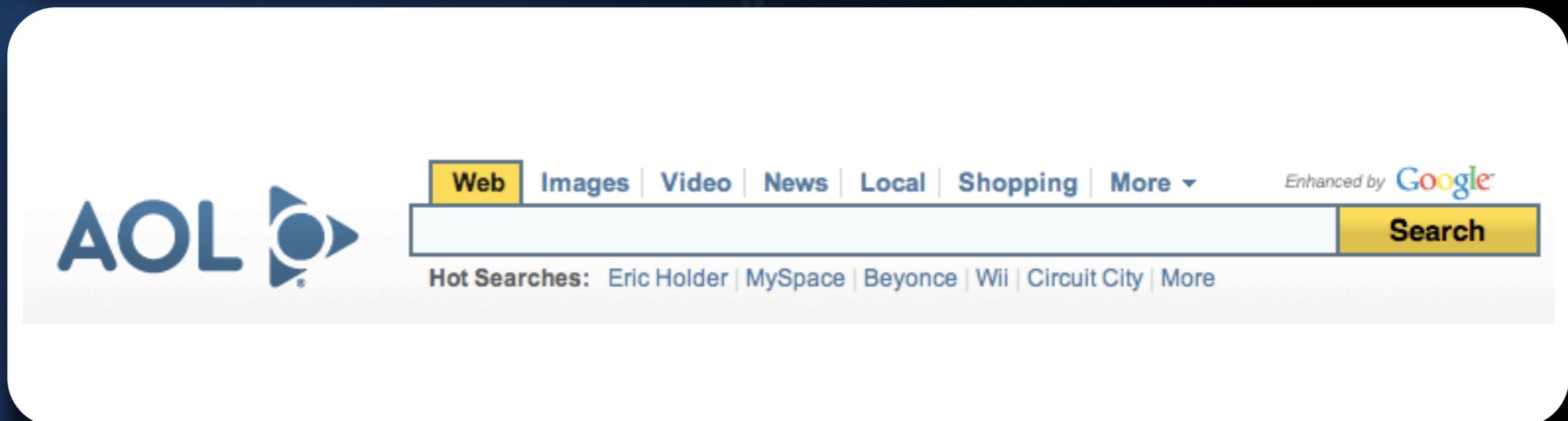
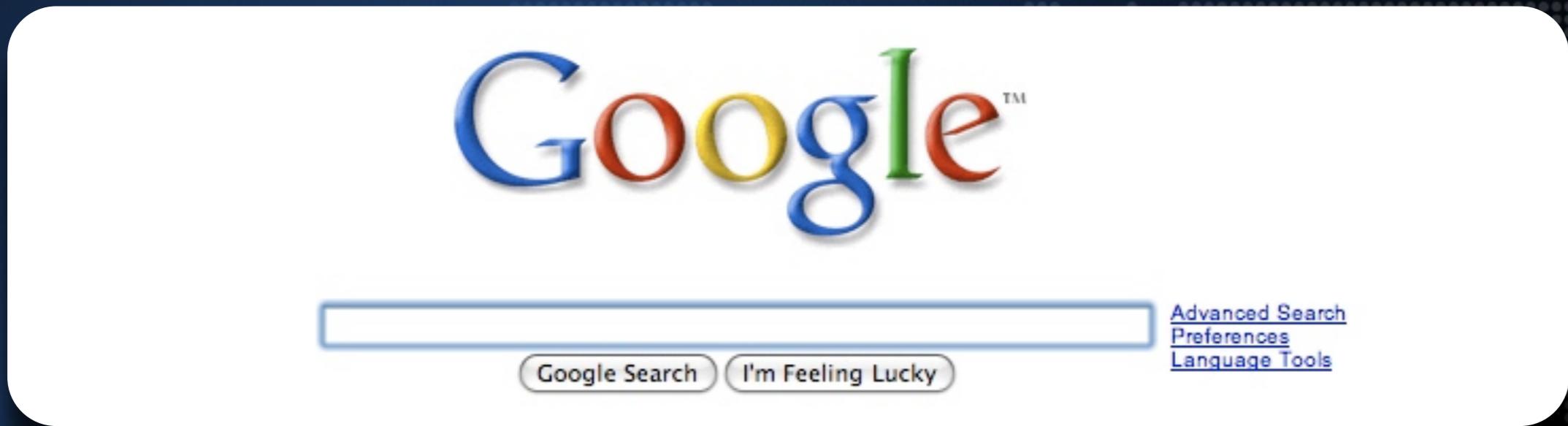
Exposed Field of Operations



The Real World is Anonymous



A Search History is Forever



www.newsweek.com

The screenshot shows a Mac OS X desktop environment. In the foreground, a web browser window displays the Newsweek website (<http://www.newsweek.com/>). The page features a large banner for 'SLUMDOG MILLIONAIRE' and a main article about the film. On the left, there's a sidebar for 'Cover Story' with an image of a person and the headline 'The Confidence Game'. On the right, there's a section for 'Latest Newsweek' with several news items. In the background, an 'Activity' window from the OS X system tray is open, showing a list of network connections and their details. One connection is highlighted, showing a URL related to the 'SLUMDOG MILLIONAIRE' banner.

Address	Status
▼ Newsweek - National News, ...and more... Newsweek.com	201 items
► http://static.coolpotters.c...elle-obama-most-recent.html	12 items
http://ad.doubleclick.net/...1;ord=233920772559940800?	1.4 KB
http://ad.doubleclick.net/...2;ord=233920772559940800?	0.4 KB
http://ad.doubleclick.net/...3;ord=233920772559940800?	0.4 KB
http://ad.doubleclick.net/...4;ord=233920772559940800?	4.6 KB
http://ads.peer39.com/adv....%20%7C%20Newsweek.com	0.3 KB
http://ads.peer39.com/advertiser/jsr/ad722.js	2.1 KB
http://bc.newsweek.com/mr...15835711&bctid=undefined	24.8 KB
http://bc.newsweek.com/players/js/bcFullscreenPlayer.js	4.4 KB
http://bc.newsweek.com/p/...moreTab=true&r=50642624	75.7 KB
http://bin.clearspring.com/lib/0.8.2/379/b.swf	21.8 KB
http://brightcove.vo.llnwd...NBC480.jpg?pubId=16991917	51.6 KB
http://brightcove.vo.llnwd...NBC480.jpg?pubId=16991917	51.6 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	14.6 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	14.6 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	12.3 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	12.3 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	16.8 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	16.8 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	15.9 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	15.9 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	20.5 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	15.6 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	15.6 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	21.9 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	21.9 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	23.6 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	23.6 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	25.1 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	25.1 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	18.7 KB
http://brightcove.vo.llnwd...00x300.jpg?pubId=16991917	18.7 KB
http://cdn.clearspring.com/...chpad/3953/preloader-en.js	21.8 KB
http://cs66.clearspring.c...&flg=800&evt=20%3D33f&s=1	67 bytes
http://edge.quantserve.com/quant.js	2.9 KB
http://js.revsci.net/gateway/gw.js?csid=j05531	4.1 KB
http://m1.2mdn.net/18432...op_012909_sb_300x250.swf	28.2 KB
http://m1.2mdn.net/879366/flashwrite_1_2.js	0.8 KB
http://m1.2mdn.net/viewad/817-grey.gif	43 bytes
http://m1.2mdn.net/viewad/817-grey.gif	43 bytes
http://media.newsweek.com/.../topTen_live/bin/top10.css	0.7 KB
http://media.newsweek.com/...ive/bin/xml/top10Data.xml	1.6 KB
http://media.newsweek.com/...rnel.swf?channel=All&nw=t	52.1 KB
http://media.washingtonpost...olex.com%3Fxto%3DAL-173?	17.4 KB
http://media.washingtonpost...house/oct/health_house.gif	3.8 KB
http://media.washingtonpost...House_ProjectGreen.gif	3.1 KB
http://media.washingtonpost...g_allergies/PG_Allergies.gif	10.8 KB
http://media.washingtonpost...ers/slate/house/jan/TH.gif	9.7 KB
http://media.washingtonpost...nks/js/utilsTextLinksXML.js	1.8 KB
http://metrics.washingtonp...ugin%20Container%3B&[AQE]	43 bytes
http://ndn.newsweek.com/me.../label_latestnewsweek.gif	0.7 KB
http://ndn.newsweek.com/site/images/get_and_share.gif	0.5 KB

The Threats

- Profiling
- Blocking
- Cloaking
- e-Identity discovery
- Hostile environments
- Malware

Profiling

- Cyber counterintelligence
- Focus of interest
- Activities
- Plans



Search & Ads

restaurants – Google Search

http://www.google.com/search?q=restaurants&ie=utf-8&oe=utf-8&aq=t&sarr=1P

restaurants – Google Search

Sites with images

More search tools

Something different

cafes

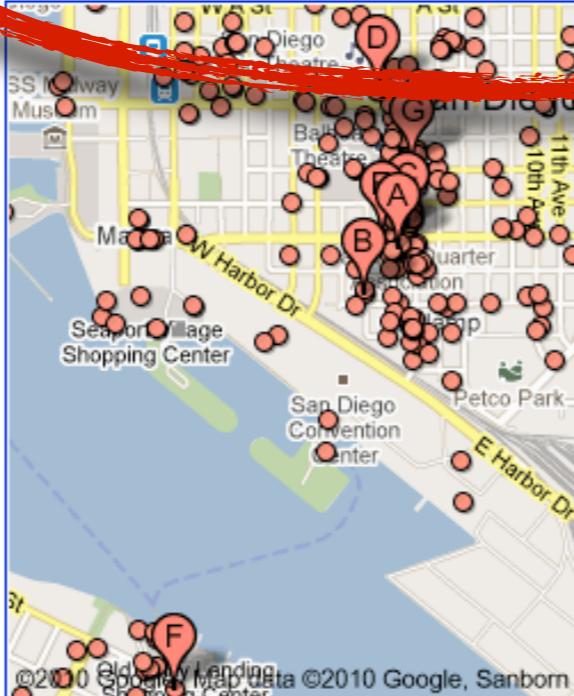
motels

night clubs

nightlife

Best Deals and Discounts on the Best Local Restaurants – Save ...
Saving money on dining out is easy with Restaurant.com gift certificates. Find restaurants in your area and get \$25 restaurant gift certificates for only \$15.
Find Restaurants - My Account - View Cart (0) - Chicago
www.restaurant.com/ - Cached - Similar

Local business results for restaurants near San Diego, CA - Change location



A Sevilla
www.cafesevilla.com - (619) 233-5979 - 12 reviews

B Candelas Restaurant
www.candelas-sd.com - (619) 702-4455 - 94 reviews

C Gaslamp Quarter Association
www.gaslamp.org - (619) 233-5227 - 23 reviews

D The Us Grant
www.starwoodhotels.com - (619) 232-3121 - 351 reviews

E Royal India - San Diego Restaurants
www.royalindia.com - (619) 269-9999 - 341 reviews

F Il Fornaio
www.ilfornaio.com - (619) 437-4911 - 78 reviews

G Croce's Restaurant & Jazz Bar
www.croces.com - (619) 233-4355 - 79 reviews

TGI Friday's®
Looking for a new place to eat?
Try Friday's Today & Get Your Flair On!
TGI Fridays.com

La Jolla Dining Guide
Restaurant Reviews, Photos, Menus Chef Profiles, Recipes, Coupons
SanDiegoRestaurants.com

Thinking of Dining Out?
Save Big on Local Restaurants with Our Discounted Gift Certificates.
www.Restaurant.com

Fine Dinning Coupons
San Diego's Best Fine Dinning Restaurant Offers
www.thebestrestaurants.com
San Diego, CA

Looking for a restaurant?
Find the best restaurants in Alaska get the latest reviews
whatsupAK.com

Restaurants
Restaurants Directory. Find It Near You!

Done

Blocking – Unprotected IP



Cloaking – American IP

الموقع العربي

[Home](#) [Site Guide](#) [Contact Us](#) [Set As HomePage](#) [Add to favorites](#)



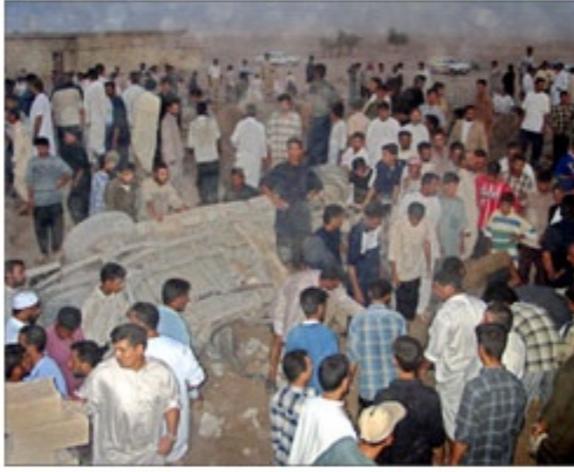
ALJAZEERA.NET

SEARCH ALJAZEERA
 Go
[Advanced Search](#)

Homepage
News
Economy
Culture
Sci-Tech
Special Reports
Weather
Polls
Your feedback
Contact Us
About Aljazeera
Frequencies
Aljazeera Mobile
News Alerts
E-marketing

Africa 04 Destinations
17 Flights per week

Updated on: Friday 23 July 2004, 19:13 Makka Time, 16:13 GMT



Fresh bombings in Falluja

US occupation forces have carried out bombings in the town of Falluja, which hospital sources say has injured five including children. [FULL STORY](#)

- Fallujans deny al-Zarqawi presence
- Fallujans: Use oil cash to rebuild homes
- Thirteen killed in US Falluja attack

Arab World [more](#) **Global** [more](#)

[Kuwait targets leading rights activist](#) [Afghan car bomb wounds four US](#)

TOP NEWS

[Turkish rail disaster stirs up a storm](#) 

[EU vows Middle East role as Israel fumes](#) 

[Al-Sadr gives first sermon in two months](#) 

[US proposes sanctions against Sudan](#) 

In pursuit of Arab Reform 

News Alerts
Subscribe / Information
Update Profile

FEATURES

Wall of contention
Israel-EU relations take a nosedive

Living in limbo
Iraq's war veterans fear being forgotten

State v teachers
Testing time for Turkish reforms

Redefining terrorism?
Question marks over China's crackdown

Cloaking – Middle Eastern IP

Indian Sub-Continent 11 Destinations

74 Flights per week

السنة الرابعة

الصفحة الرئيسية | مركز المساعدة | Help center | إلى الجزيرة

كيف تقرأ العربية

السبت 7/6/1425هـ الموافق 24/7/2004م (آخر تحديث) الساعة 02:06 (مكة المكرمة), 23:06 (غرينتش)

Now in English english.aljazeera.net

ابحث في الجزيرة نت

ابحث

بحث تفصيلي

المشاركة التفاعلية

البريد الإلكتروني

كلمة المرور

دخول

مشاركة جديد

امتيازات عضوية

الموقع

تسريب كلمة المرور

اقرأ في الجزيرة نت

الفدرالية الدولية

حقوق الإنسان

نهضة العرب العلمية

Middle East 04 Destinations

21 Flights per week

الأخبار

الاقتصاد والأعمال

العلوم والتكنولوجيا

الطب والصحة

الرياضة

الثقافة والفن

جولة الصحافة

قضايا وتحليلات

ملفات خاصة

كارикatur

كتب

وجهات نظر

الفاعلات الحية

تصويت

منتديات الجزيرة

مركز التدريب والتطوير



الجزيرة نت

aljazeera.net

السنة الرابعة

دبلوماسي أمريكي يؤكد أن الرأس المقطوع
آخر التطورات

بماذا تبرر الاهتمام الدولي
المترادف بدارفور؟
 تفادي كارثة إنسانية
 استجابة لضغط
 أميركية
 أخرى

مدة التصويت
من 2004/07/23
إلى 2004/07/26

نتائج
شارك

اختطاف دبلوماسي مصرى في بغداد

قال وزير الخارجية المصري الأحمد أبو الغيط إن بلاده لن ترسل أي قوات على العراق، وذلك ردًا على خطف مجموعة مسلحة أحد دبلوماسيها في بغداد. في غضون ذلك أمهلت جماعة مسلحة أخرى تحتجز سبعة رهائن 48 ساعة للشركة الكويتية التي تتطلبهم لاستجابة لمطالبيها... الفضيل

Pricing through the standard IP on hotels.com is \$91 less expensive than the pricing through the Geo Distribution IP

New York City Hotels - New York Hotel Discounts - hotels.com - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Favorites Home Options

Address http://www.hotels.com/promotion.jsp?id=1039

Google Search Web AutoFill Options

Alexa Search Info 433 All-hotels Hotel Motel And Condo Finder A... Arabian Gulf Hotel

The Hotel Thirty Thirty is situated on the East Side of Manhattan, between Madison and Park Avenues. [more...](#)
[map](#) | [hotel information](#)

On The Ave Hotel
 Upper West Side / New York
 Located on the Upper West Side of Manhattan, On The Ave is a sophisticated but reasonably priced hotel that stands close to the Lincoln Center, Hayden Planetarium, Museum of Natural History, Broadway [more...](#)
[map](#) | [hotel information](#)

Holiday Inn Midtown 57th St
 2 Blocks From Central Park / New York City
 The Holiday Inn Midtown has an outstanding location in a quiet residential neighborhood, in the otherwise, bustling Midtown Manhattan. [more...](#)
[map](#) | [hotel information](#)

Park Central New York
 Across From Carnegie Hall / New York
 The Park Central Hotel New York is located in the heart of in Midtown Manhattan directly across from Carnegie Hall. [more...](#)
[map](#) | [hotel information](#)

Hotel Chandler, Frm Le Marquis
 Off 5th Ave/Murray Hill / New York
 One of New York City's newest luxury boutique hotels nestled in historic Murray Hill, the Hotel Chandler, Frm Le Marquis stands close to the United Nations and the Garment and Flatiron districts of sh... [more...](#)
[map](#) | [hotel information](#)

The Time Hotel
 Broadway Half A Block / New York
 The Time Hotel is located in the heart of Manhattan's Times Square, placing Hotels.com travelers close to everything: nearly 40

from \$172.00 Until Jul 20 [SELECT](#)

from \$179.00 Until Jul 20 [SELECT](#)

from \$179.00 Until Jul 20 [SELECT](#)

from \$205.00 Until Jul 20 [SELECT](#)

from \$249.00 Until Jul 20 [SELECT](#)

info.alexa.com/data/details?url=http%3A//www.hotels.com/promotion.jsp%3Fid%3D1039

Standard IP: \$179 (EU 139)

hotels.com -- globale korting hotel reserveringen - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Search Web Options

Proxy: International Route Apply Edit Remove Add Status: Using International Route Options

502 Bad Gateway

YORK
 Situated close to infinite options for dining, shopping and entertainment, the Millennium Broadway stands only a half block from glittery Times Square in the middle of the lights of Broadway. [meer...](#)
[kaart](#) | [Hotelinformatie](#)

Holiday Inn Midtown 57th St
 2 BLOCKS FROM CENTRAL PARK / NEW YORK CITY
 The Holiday Inn Midtown has an outstanding location in a quiet residential neighborhood, in the otherwise, bustling Midtown Manhattan. [meer...](#)
[kaart](#) | [Hotelinformatie](#)

The New York Helmsley Hotel
 42ND/3RD / NEW YORK
 Midtown Manhattan's New York Helmsley Hotel offers an undisputedly great location, cosmopolitan feel and sophisticated ambience, making the famously named facility a favorite with guests from through [meer...](#)
[kaart](#) | [Hotelinformatie](#)

Carlton New York
 GRAMERCY/MADISON SQUARE PARK / NEW YORK
 As New York's newest grand old hotel, the Carlton stands between the Murray Hill and Gramercy Park neighborhoods, where tree-lined streets make guests feel they're staying at a house rather than the c... [meer...](#)
[kaart](#) | [Hotelinformatie](#)

Alleen beschikbaar!

Gemiddelde tarief per nacht 1 jun 2 jun

€ 211,50	€ 164,00	€ 259,00
----------	----------	----------

kiezen

Gemiddelde tarief per nacht 1 jun 2 jun

€ 186,00	€ 186,00	€ 186,00
----------	----------	----------

kiezen

Gemiddelde tarief per nacht 1 jun 2 jun

€ 207,00	€ 207,00	€ 207,00
----------	----------	----------

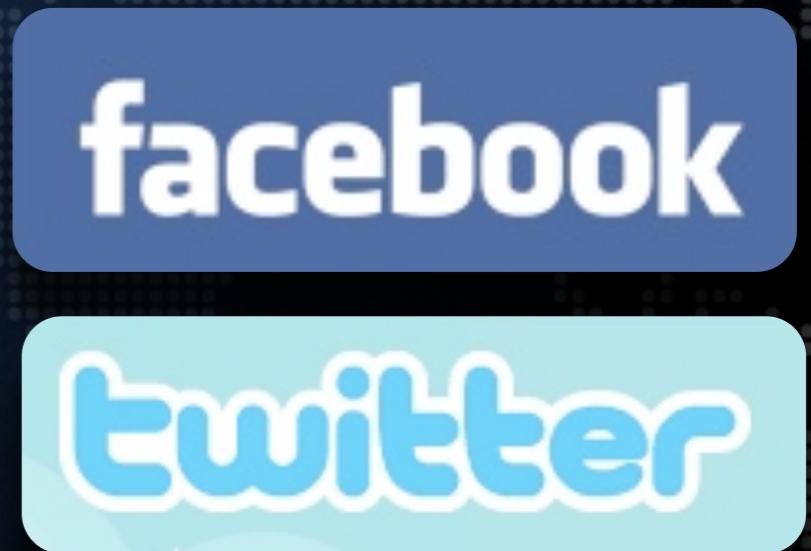
Alleen beschikbaar!

kiezen

Geographic Distribution IP: \$270 (EU 211)

e-Identity Discovery

- Extended duration
- High visibility
- Google background



A screenshot of a Google search results page. The search bar contains the query "clark kent". The results section shows a link to the first result, which is a Web page titled "Results 1 - 10 of about 2,970,000 for clark kent. (0.14 seconds)".

Google™ clark kent Search Advanced Search Preferences

Web Show options... Results 1 - 10 of about 2,970,000 for clark kent. (0.14 seconds)

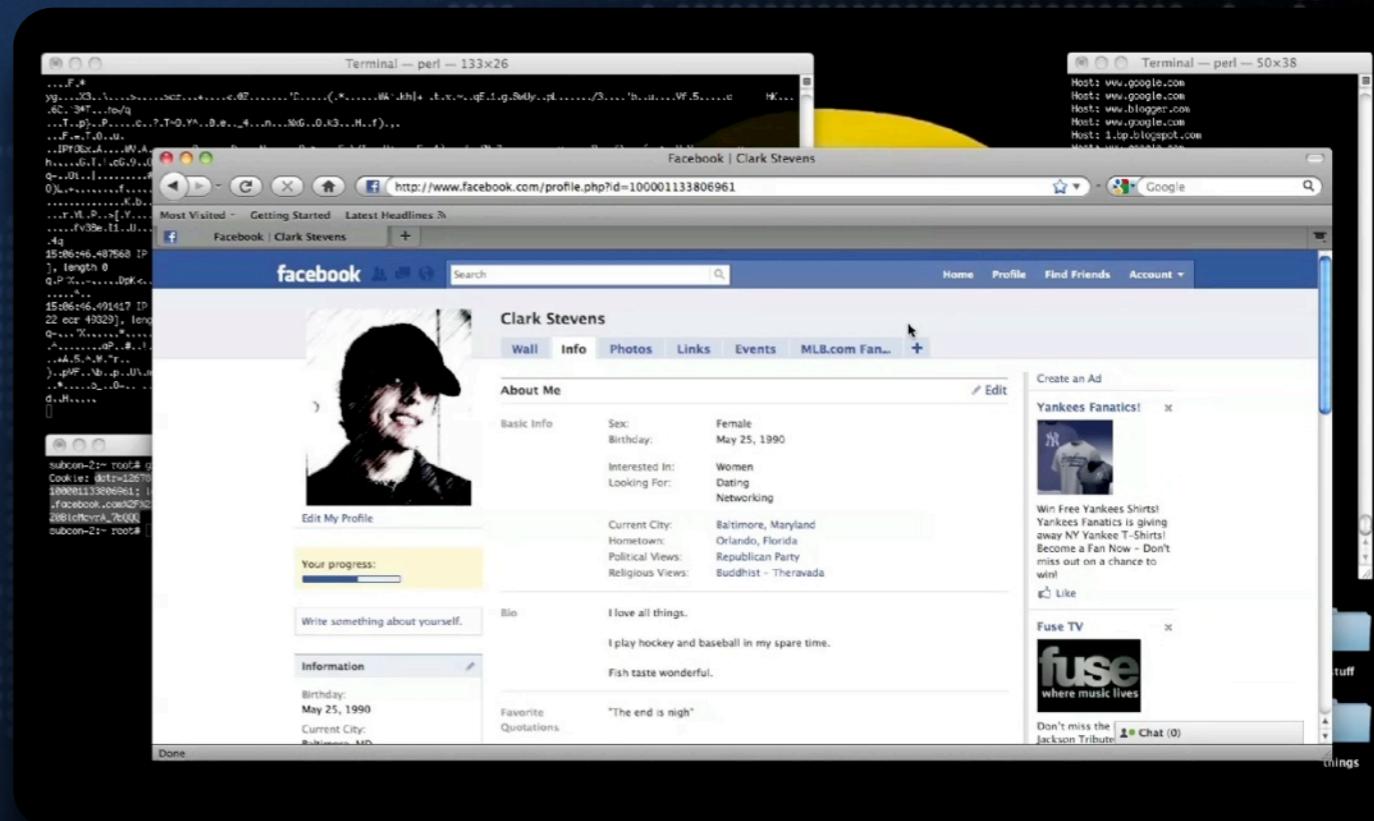
Hostile Environments

- Traffic analysis
- Forensics
(capture of physical hardware)



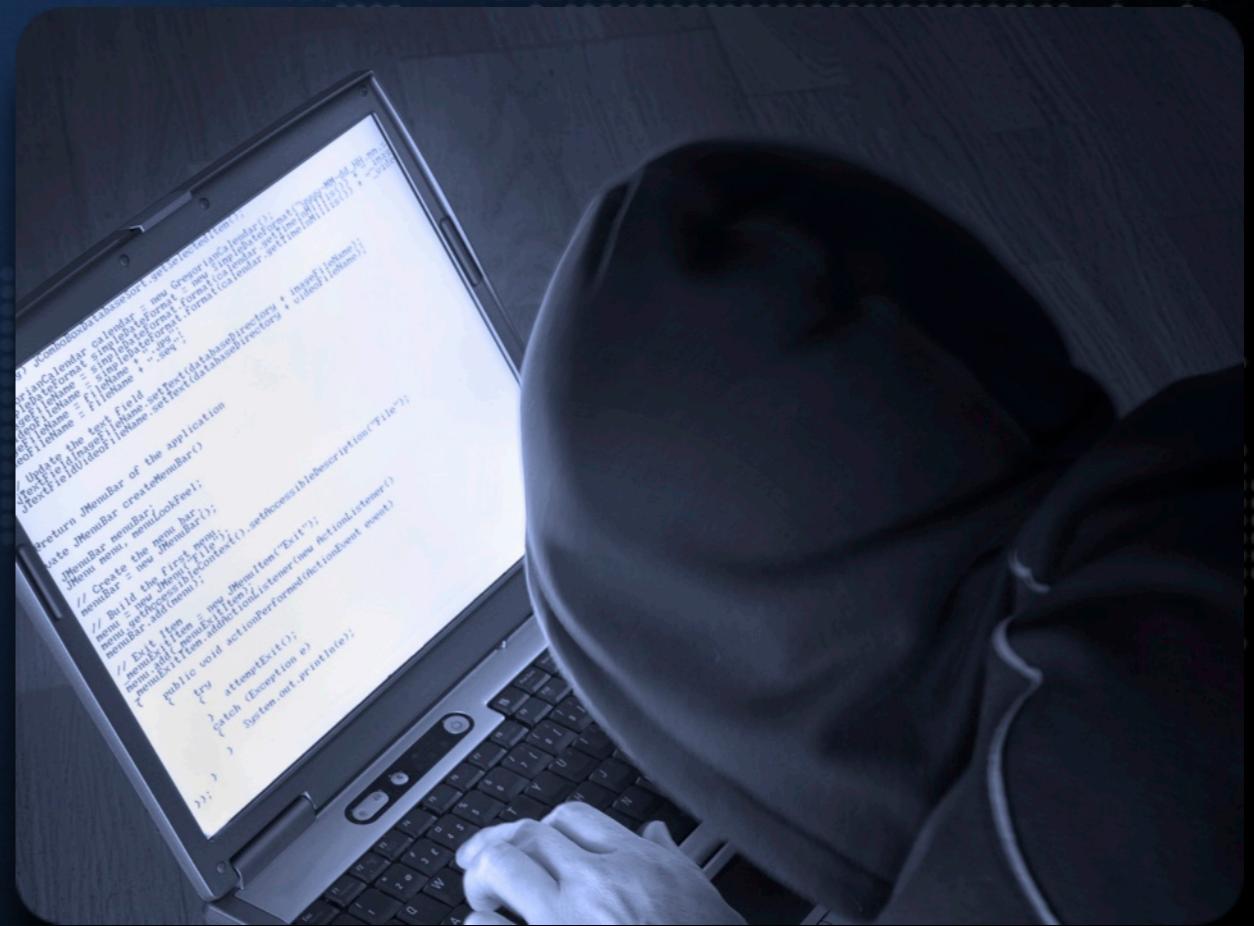
Facebook Hijack

- Anyone at an open Wi-Fi can read all of your unencrypted traffic
- Attacker can intercept personal information
- Attacker can capture and use:
 - Username
 - Password
 - Authentication cookies



Malware

- Exposed Internet activities leave internal networks vulnerable to compromise





How do they know?

What is an IP address?

Your computer's
“street address”
on the Internet

97.65.188.109



WHOIS

Name: **DRUG ENFORCEMENT ADMIN-DJDEA**
Address: **800 K STREET #500**
City: **WASHINGTON**
State: **DC**
Postal Code: **20091**
Country: **US**
Reg Date: **2008-10-16**
Updated: **2008-10-16**
Net Range: **209.183.199.128 - 209.183.199.143**
Org Tech Name: **Network Operations Center**
Org Tech Phone: **+1-301-589-3060**
Org Tech Email: **noc@atlantech.net**

Published IP Addresses

Blocklist Manager

The screenshot shows the Blocklist Manager application window. The menu bar includes File, Edit, Clear, Import, Export, Array, Tools, Donate, and Help. Below the menu is a toolbar with icons for Sources, Process, Add IP, Import List, Export List, Convert, Whois, Options, and Exit. The main area is a table with columns: Range Start, Range End, Rule T..., Comment, Sources, IP Count, Netmask, and CIDR. The table lists numerous IP address ranges and their associated details, such as Deny rules for various organizations like DHL Systems Inc, DHS, and DHS CUSTOMS & BORDER PROTECTION.

Range Start	Range End	Rule T...	Comment	Sources	IP Count	Netmask	CIDR
207.078.063.000	207.078.063.255	Deny	DHL Systems Inc	PG	00000000256	255.255.255.000	/23
209.078.057.240	209.078.057.255	Deny	DHL Systems Inc	PG	00000000016	255.255.255.240	/23
198.141.000.000	198.141.255.255	Deny	DHL Systems, Inc, DHL Systems Inc	PG	00000065536	255.255.000.000	/16
194.219.092.064	194.219.092.079	Deny	Dhmos Kalymnou	PG	00000000016	255.255.255.240	/23
062.001.018.064	062.001.018.079	Deny	dhmos pallinis	PG	00000000016	255.255.255.240	/23
067.135.067.016	067.135.067.023	Deny	DHS	PG	00000000008	255.255.255.248	/23
212.042.178.016	212.042.178.023	Deny	DHS	PG	00000000008	255.255.255.248	/23
075.144.113.032	075.144.113.047	Deny	DHS - FLETC	PG	00000000016	255.255.255.240	/23
075.145.200.088	075.145.200.095	Deny	DHS - FLETC-FRI	PG	00000000008	255.255.255.248	/23
012.032.098.240	012.032.098.255	Deny	DHS CLUB INC	PG	00000000016	255.255.255.240	/23
069.225.166.128	069.225.166.135	Deny	DHS CUSTOMS & BORDER PROTECTION-040811045247	PG	00000000008	255.255.255.248	/23
069.233.188.216	069.233.188.223	Deny	DHS CUSTOMS & BORDER PROTECTION-041201033537	PG	00000000008	255.255.255.248	/23
069.230.001.016	069.075.144.113.032	069.075.144.113.047	Deny	DHS - FLETC			
065.005.094.064	065.005.094.079	075.145.200.088	075.145.200.095	Deny	DHS - FLETC- FRI		
076.216.109.200	076.216.109.207	012.032.098.240	012.032.098.255	Deny	DHS CLUB INC		
076.249.166.208	076.249.166.209	069.225.166.128	069.225.166.135	Deny	DHS CUSTOMS & BORDER PROTECTION		
063.086.100.232	063.086.100.233	069.233.188.216	069.233.188.223	Deny	DHS CUSTOMS & BORDER PROTECTION		
196.012.174.000	196.012.174.001	069.230.001.016	069.230.001.023	Deny	DHS CUSTOMS & BORDER PROTECTION		
076.205.227.232	076.205.227.233	065.005.094.064	065.005.094.079	Deny	DHS Ft McCellan		
076.228.020.088	076.228.020.089	065.005.094.064	065.005.094.079	Deny			
012.004.029.240	012.004.029.241	065.120.069.000	065.120.069.001	Deny			
065.120.069.000	065.120.069.001	067.133.227.048	067.133.227.049	Deny			
067.133.227.048	067.133.227.049	067.135.189.128	067.135.189.129	Deny			
067.135.189.128	067.135.189.129	203.148.208.000	203.148.208.001	Deny			
203.148.208.000	203.148.208.001	203.154.068.000	203.154.068.001	Deny	Dhurakijpundit University	0000000512	255.255.254.000
203.154.068.000	203.154.068.001	203.155.120.000	203.155.121.255	Deny	Dhurakijpundit University	PG	0000000512
203.155.120.000	203.155.121.255	221.128.120.000	221.128.121.255	Deny	Dhurakijpundit University	PG	0000000512
221.128.120.000	221.128.121.255	081.092.045.144	081.092.045.151	Deny	DI CLEMENTE SOFTWARE	PG	00000000008
081.092.045.144	081.092.045.151	217.222.020.168	217.222.020.175	Deny	DI DEDDA ELETTROMEDICALI	PG	00000000008
217.222.020.168	217.222.020.175	085.044.040.232	085.044.040.239	Deny	DI IORIO ITALO FRANCESCO	PG	00000000008
085.044.040.232	085.044.040.239	063.192.199.128	063.192.199.135	Deny	Di Napoli J Phillip Atty	PG	00000000008

Exposed IP Addresses

- Total IP addresses worldwide:
Over 4 billion
 - IP addresses tracked on monitored lists:
Over 2.5 billion
- 59%** of all IPs are published

Source: Blocklist Manager

Geolocation

Based on:

- IP address
- GPS
- Cell Towers
- Wi-Fi
- Behavior



Illegal Anonymity is Easy

- Buy access with stolen credit card
- Use stolen access account
- Bot Net
- Malware/Phishing



Non-Attribution is Not Enough



Overt Attribution



Zero Attribution



Blend In

Philosophical Approach

- Look like them
- Act like them
- Leave no unintended patterns
- Isolate research network from analysis
- Consider how you look at your end as well as to targets

Non-Attribution Looking Like Nobody In Particular

- Usually geographically specific
- No particular identity
- Minimize patterns
- Techniques
 - Random identities
 - Long recurrence
 - Wipe history



High Volume Non-Attribution Hiding the Spotlight

- Automated search or harvesting generates massive traffic
- Detectable even if non-attributed
- **Key metric**
 - Hits per target per source per day
- **Techniques**
 - Many sources
 - Rate limited
 - Human-like click patterns

Misattribution Working in Alias

- Communications are trackable to a specific entity
- Long lifetime aliases require special treatment
- Born yesterday problem



Location Non-Attribution

- Second biggest targeting factor (after identity)
- Must look like a local
When in Rome....
- Technical and human blending
- Which social networking site?
- Which chat rooms?

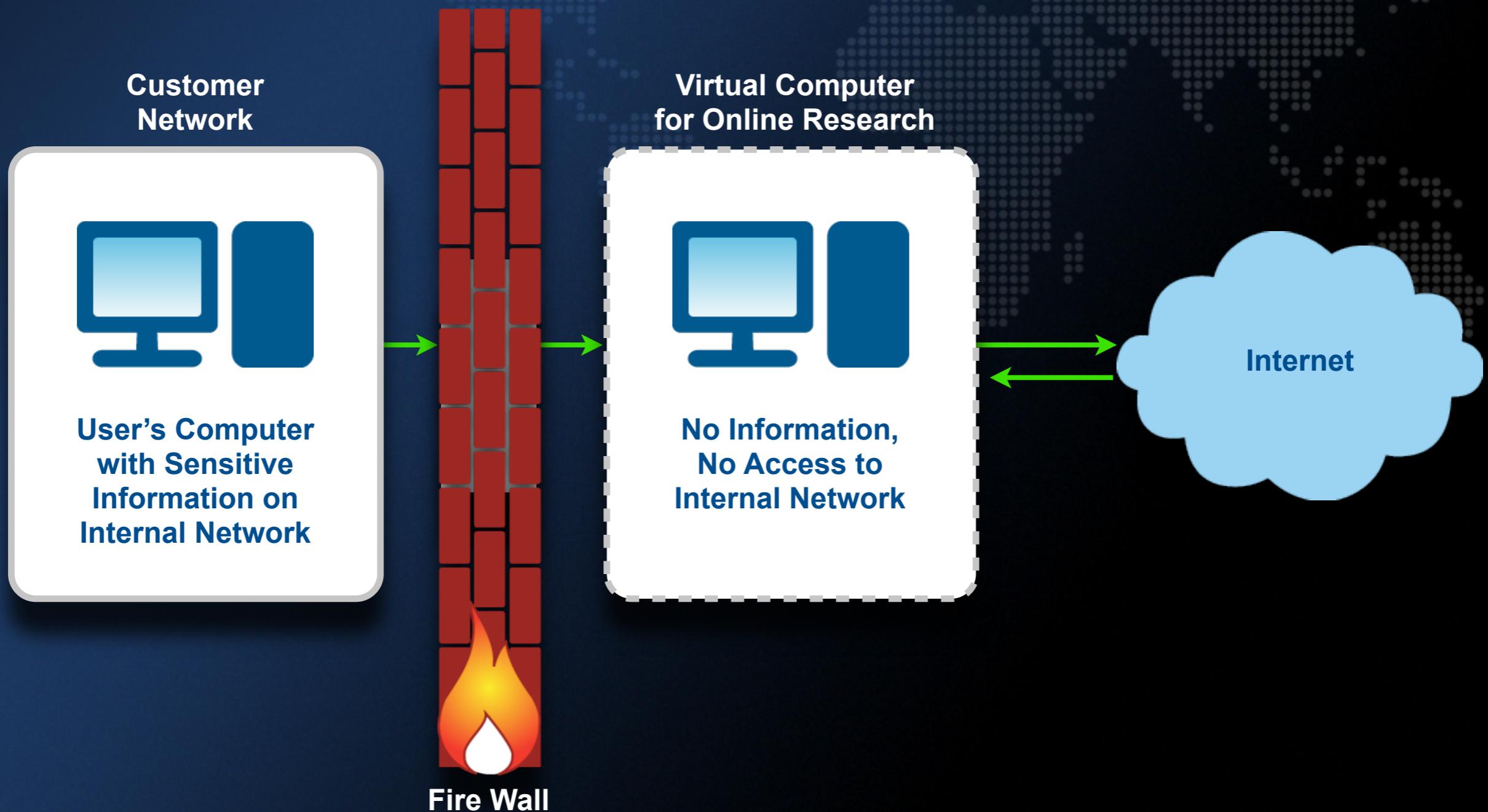


HTTP Metadata

System capable of changing:

- Country or region of origin
- Language
- Character set
- Operating system
- Browser type and version

Isolate Your Activity From Your Network



Best Practices to Protect Yourself

1. Think before you type. Your brain is your best security tool.
2. Use a different email address for every website and for each activity.
3. Use unique usernames and passwords for every site and for each activity.
4. Clear private data and history from your browsers after every session.
5. Use and maintain firewall and anti-malware tools.
6. When engaged in Web harvesting, use a large number of source IP addresses.
7. Do not conduct any personal business on operational computers.
8. Work in a virtualized environment, and revert to a baseline image frequently.
9. Never keep sensitive or work information on the machine (or Virtual Machine Image) used for Internet operations/investigations.
10. Make sure your Internet activities can never be traced back to you or your organization.

Thank You

Lance Cottrell
CTO, Ntrepid
lance.cottrell@ntrepidcorp.com

Exhibit Booth #209