



Tenacious Diggity

Skinny Dippin' in a Sea of Bing

29 July 2012 – DEF CON 20 – Las Vegas, NV



Presented by:
Francis Brown & Rob Ragan
Stach & Liu, LLC
www.stachliu.com

Agenda

OVERVIEW

- Introduction/Background
- Advanced Attacks
 - **NEW** Diggity Attack Tools
- Advanced Defenses
 - **NEW** AlertDiggity Cloud Database
- Future Directions

Introduction/Background

GETTING UP TO SPEED



Diggity Tools

PROJECT OVERVIEW



GOOGLE HACKING DIGGITY HISTORY OF GOOGLE HA

History of Google Hacking

Timeline Flipbook List Map

Timeline of Google Hacking events:

- 2006: Bing tool released by Blueinfy (Nov 2005)
- 2007: Google Hacking v2 released (Nov 2, 2007)
- 2008: cDc Goolag - gui tool released (Mar 2008)
- 2009: FoundStone SiteDigger v 3.0 released (Dec 1, 2009)
- 2010: Stach & Liu Unveils Google/Bi (Jul 29, 2010)

RESOURCES GOOGLE HACKING DIGGITY PROJECT

Google Hacking Diggity Project

The Google Hacking Diggity Project is a research and development initiative dedicated to investigating the latest techniques that leverage search engines, such as Google and Bing, to quickly identify vulnerable systems and sensitive data in corporate networks. This project page contains downloads and links to our latest Google Hacking research and free security tools. Defensive strategies are also introduced, including innovative solutions that use Google Alerts to monitor your network and systems.

DEFENSE TOOLS

ATTACK TOOLS

PRESENTATION SLIDES



Diggity Tools

ATTACK TOOLS



Tool	Description
GoogleDiggity	Traditional Google hacking tool
BingDiggity	Bing equivalent of traditional Google hacking tool
FlashDiggity	Adobe Flash security scanning tool
DLPDiggity	Data loss prevention scanning tool
LinkFromDomain	Bing footprinting tool based on off-site links
CodeSearch Diggity	Open-source code vulnerability scanning tool
MalwareDiggity	Malware link detection tool for off-site links

Diggity Tools

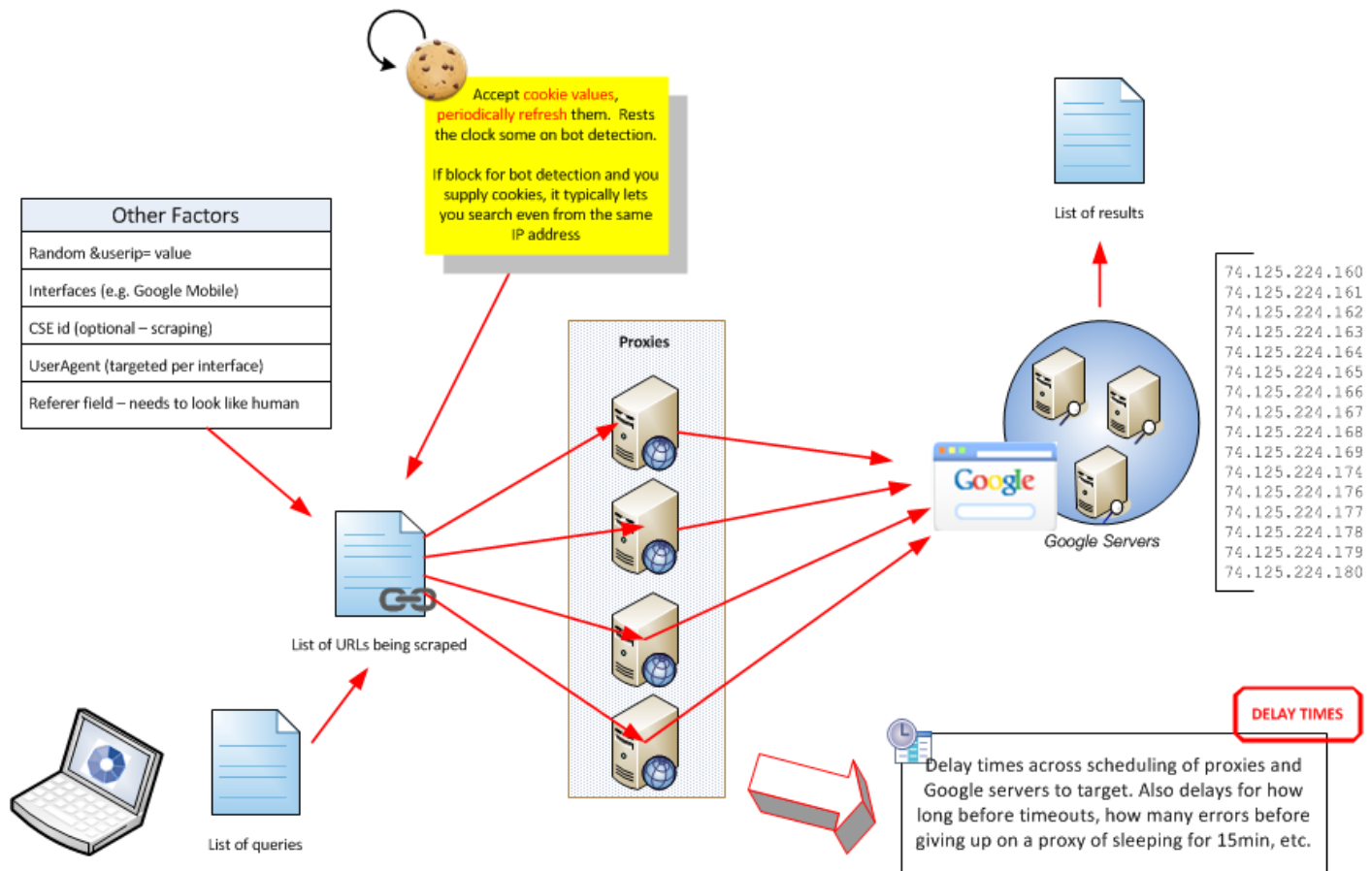
NEW ATTACK TOOLS



Tool	Description
PortScan Diggity	Passive port scanning via Google
NotInMyBackYard	Easily find your info in third-party sites
BHDB 2.0	New Bing Hacking DB now as affective as Google
Bing BinaryMalware	Find malware via Bing's indexing of executables
CodeSearch REBORN	Brought back from the dead
SHODAN Diggity	Easy interface to SHODAN search engine

Diggity Scraping

NEW ACROSS ALL ATTACK TOOLS



Diggity Scraping

PROXIES SPECIFICATION

Auto Proxies

Add Auto-Find Test Purge Testing proxies...

Bad: (36)

- http://60.12.193.47:8090
- http://211.154.83:5:80
- http://60.10.58.3:8090
- http://222
- http://124
- http://58.2
- http://119.73.47.165:8118
- http://119.73.74.222:8118

Untested: (15)

- http://121.110.15.100:80 Testing...
- http://211.151.152.108:80 Testing...
- http://92.9.15.89:8118 Testing...
- htt Testing...
- htt Testing...
- http://124.195.6.243:8080 Pending...
- http://92.96.205.66:8118 Testing...
- http://189.39.115.174:3128 Pending...

Good: (249)

- http://200.32.64.235:8080
- http://189.80.20.187:8080
- http://113.105.85.6:8080
- http://61.152.106.203:8080
- http://200.58.199.50:8080
- http://119.30.112.212:8080
- http://171.101.111.232:3128
- http://177.69.203.242:8080

Search Diggity

File Options Help

Google

Reset

Clear Results

Settings

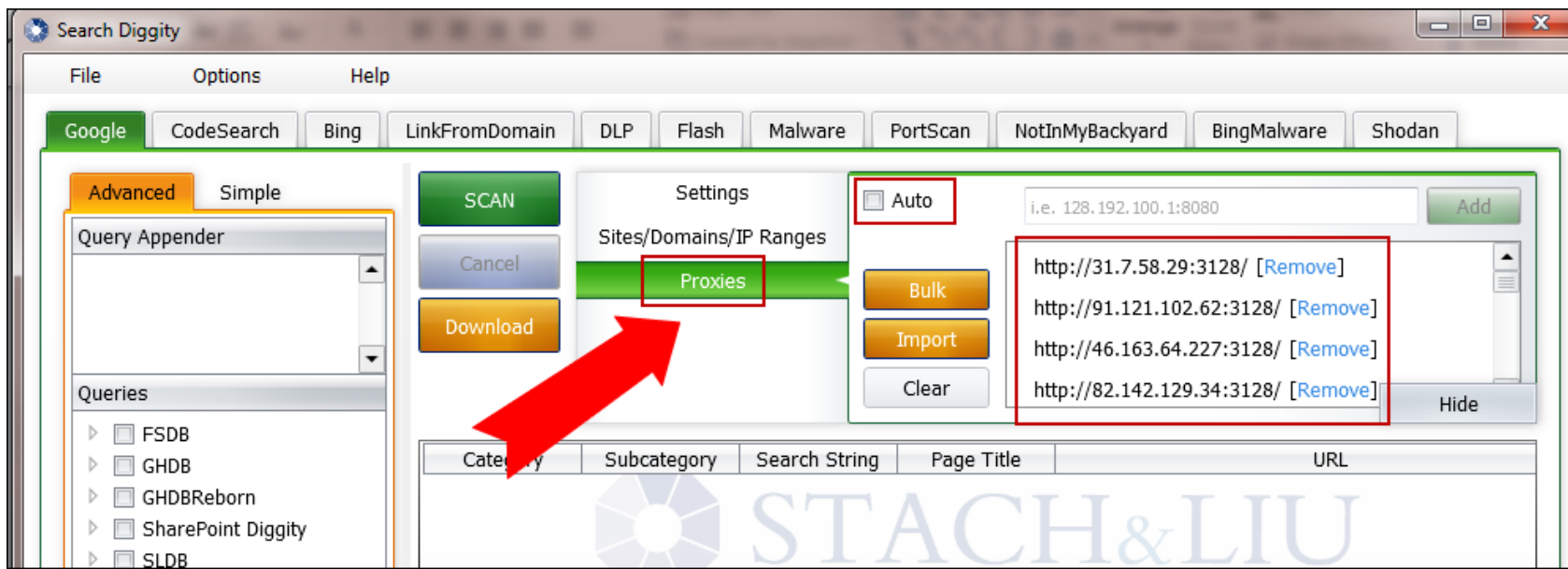
Proxies

Automatically find open web proxies to use

Test to ensure proxies are actually working and are fast

Diggity Scraping

MANUAL PROXIES SPECIFICATION



Advanced Attacks

WHAT YOU SHOULD KNOW



NEW GOOGLE HACKING TOOLS

PortScan Diggity

PortScanning

TARGETING HTTP ADMIN CONSOLES

Searching for web admin interfaces on non-standard HTTP ports

The image displays two screenshots of Google search results. The left screenshot shows a search for `site:/com:*` with a callout box stating "All non-port 80/443 HTTP admin consoles for .com". The right screenshot shows a search for `site:/216.75.*.*` with a callout box stating "IP address range search for HTTP admin interfaces on non-standard ports". Both screenshots show search results for various websites with non-standard ports highlighted in yellow.

Search Query	Results	Highlighted URLs
<code>site:/com:*</code>	About 681,000 results (0.06 seconds)	https://www.twimbow.com:5223/ https://tribe.vastspot.com:81/ https://davidsonsmotors.com:1644/
<code>site:/216.75.*.*</code>	16 results (0.06 seconds)	216.75.63.101:9998/ 216.75.172.130:8015/ 216.75.20.82:32000/mail/

PortScanning

TARGETING PORT RANGES

Searching for specific port ranges

Google search results for the query `site:/com:* 8000..9000`. The search bar contains the query, and a callout box points to it with the text "Targeting ports 8000-9000". The search results show "About 399,000 results (0.40 s)". The left sidebar includes "Web", "Images", "Maps", "Videos", "News", "Shopping", and "More". The main results list:

- Webcams - BC Ferries:**
orca.bcferrys.com:8080/cc/conditions/cams.asp
Webcams at our Major Terminals. Conditions at a glance
Terminal Traffic Outside Terminal. Traffic to Nanaimo (Dul)
- My account | BT Wi-fi**
<https://www.btopenzone.com:8443/>
BT Openzone is now BT Wi-fi. Enjoy great-value wi-fi bro
Wi-fi.
- 2012 Trinity River Photo Contest - the City of [unclear]**
weborigin1.dallascityhall.com:8080/trinityContest/
Welcome to the 2012 Photo Contest. What does it take

Google search results for the query `site:/com:* 5000..6000`. The search bar contains the query, and a callout box points to it with the text "Port scan 5000-6000". The search results show "About 216,000 results (0.40 s)". The left sidebar includes "Web", "Images", "Maps", "Videos", "News", "Shopping", and "More". The main results list:

- Live Demo - Synology**
demo.synology.com:5000/
- Discworld Mud**
discworld.imaginary.com:5678/
Discworld MUD is a multiplayer, text-based onl
as written by Terry Pratchett. On Discworld you
- FreeTranslation.com**
ets.freetranslation.com:5081/

PortScanning

TARGETING VULNERABILITY

Targeting specific HTTP ports example

Google search results for the query `site:/com:8443/`. The search returned approximately 65,900 results in 0.12 seconds. The results include:

- Parallels Plesk Panel 9.5.4**
<https://casablancareus.com:8443/>
Iniciar sesión en Parallels Plesk Panel "Nombre de usuario" y la contraseña e
- Parallels Plesk Control Panel 8.**
<https://www.gustalis.com:8443/>
Se connecter à Parallels Plesk Control passe dans les champs "Login" et "Mo
- Narmada: eWebGuru Plesk Par**
<https://99birthday.com:8443/>
Log in to Parallels Plesk Panel 9.5. En the "Password" field, press the Tab

Found ~66k targets for Plesk Panel exploit

Krebs on Security
In-depth security news and investigation

Plesk 0Day For Sale As Thousands of Sites Hacked

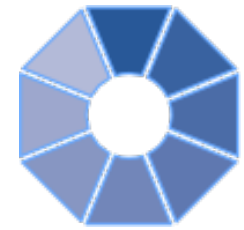
247 tweets
retweet

Hackers in the criminal underground are selling an exploit that extracts the master password needed to control **Parallels' Plesk Panel**, a software suite used to remotely administer hosted servers at a large number of Internet hosting firms. The attack comes amid reports from multiple sources indicating a spike in Web site compromises that appear to trace back to Plesk installations.

A miscreant on one very exclusive cybercrime forum has been selling the ability to hack any site running Plesk Panel

Plesk Panel Multiple Exploits all versions <= 10.4.4

PortScan Diggity



TARGETING HTTP ADMIN CONSOLES

Lists open ports per host

Host	Open
radioexercitocelstial.com	7002
fnoobradio.com	8092; 8100
www.stottpilates.com	16080
dancefoxcomet.com	8495
deepeyeradio.com	8006; 8058
radio9975.com	8002

Looking for open ports on *.com

Search String	Domain	Port	Page Title	URL
site:/com:*	ponelemusica.com	8024	SHOUTcast Adr	http://ponelemusica.com:8024/
site:/com:*	metronicfm.com	8030	SHOUTcast Adr	http://metronicfm.com:8030/
site:/com:*	manage-golf.com	8084	Manage Golf Sy	http://montrose.manage-golf.com:8084/
site:/com:*	zoukizomba.com	8052	SHOUTcast Adr	http://zoukizomba.com:8052/
site:/com:*	ebengaliradio.com	7509	SHOUTcast Adr	http://www.ebengaliradio.com:7509/
site:/com:*	mgoblog.com	8080	mgoblog Mich	http://mgoblog.com:8080/



NEW GOOGLE HACKING TOOLS

NotInMyBackYard



Data Leaks on Third-Party Sites

SENSITIVE INFO EVERYWHERE

Verizon - 2012 Data Breach Investigation Report

External breach notification methods are much different for large organizations. While notification by law enforcement was the second most seen, at 10%, it was still far lower than that of the overall dataset. In most cases for large organizations notification occurred when the thief made the disclosure known. Perhaps we should create new breach discovery classifications of “YouTube,” “Pastebin,” and “Twitter” for the 2013 DBIR? (Of course, we’re joking (sort of), but it is quite important to understand the role social networking plays in breach discovery, but also in how attacks are initiated using these tools. Perhaps we’ll follow up with a blog post another time.) An interesting “what-if” scenario would be whether or not these organizations would have discovered these breaches through some sort of internal breach discovery method. In many cases, there is little evidence suggesting they would.



PasteBin Leaks



PASSWORDS IN PASTEBIN.COM POSTS

- Twitter feed tracking passwords leaked via PasteBin

The image shows a Twitter feed on the left and a PasteBin post on the right. The Twitter feed features the account 'PastebinLeaks' (@PastebinLeaks) with a bio: 'Glued to the leak Discovering leaks on Pastebin, web attacks and so on'. Two tweets are visible, both mentioning 'Possible Massive mail/pass leak' and 'Possible listing of http passwords'. A red callout bubble points to the tweets with the text: 'Twitter feed tracking public data leaks via PasteBin.com'. The PasteBin post is titled 'http://biclopsgames.com (hacked)' and contains a list of database records. A red callout bubble points to the records with the text: 'Usernames, emails, and password hashes of compromised website posted to PasteBin.com'. The records are as follows:

username	user_password	user_email
\$voloch	b35d1ac9729539d9f8ef87508e8b2be0	kirillwow79@mail.ru
海盗	5e0ed8d03d765e4fb5128b6ba7bc8481	
AaronFF	cee3d5a7af23179acea3550fc6301300	EmbeveIcomo@mail.bij.
abadrabPype	1e3c47bf39af11993cfdc689693b7012	jeinso.n.wels
absurdism	297dbe7699dcfa60609bf9e667e2e4dc	evolancia@gmail
Accichfueve	adefb16336d900168c9bfc40af5b18ef	lokorepaserna

Cloud Docs Exposures

PUBLIC CLOUD SEARCHING



Dropbox

Google docs

Public cloud storage document exposures

Google search results for the query: `intext:"name" intext:"address" intext:"taxpayer" site:dl.dropbox.com`. The search returned 7 results in 0.23 seconds. A callout bubble points to the search query with the text: "Looking for sensitive data leaks in Dropbox cloud storage". One result is highlighted: a PDF file named "... W-9" located at `https://dl.dropbox.com/s/.../CTMUN_W9_Request_For_TaxID.pdf?...`. A second search is shown below, with the query: `site:live.com "skydrive" ext:dmp`. A callout bubble points to this search with the text: "Database dump files on Microsoft SkyDrive". The results for this search include "Windows Live SkyDrive" links to files like `https://skydrive.live.com/embedicon.../Open 060510-38688-01.dmp` and `https://skydrive.live.com/embedicon.../Open 122509-26520-01.dmp`.

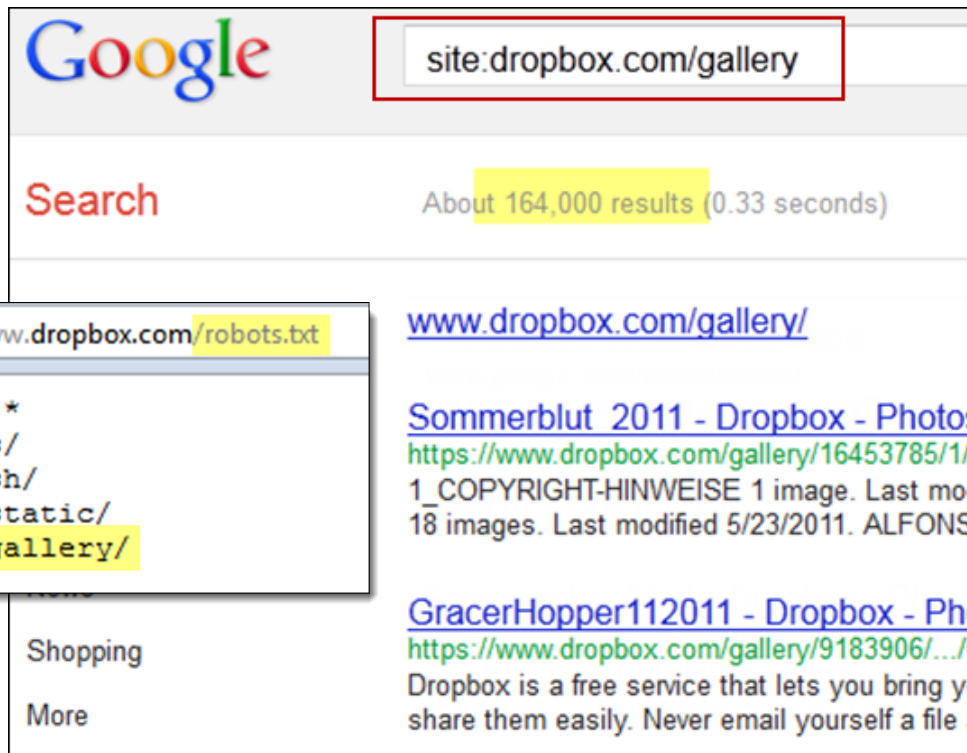
Google search results for the query: `intext:"enable password" inurl:docid site:docs.google.com`. The search returned 4 results in 0.13 seconds. A callout bubble points to the search query with the text: "Cisco config files with passwords in Google Docs files". The results include several Google Docs links, such as `https://docs.google.com/View?docid=0AbKTT...1...1...`. One result snippet is highlighted, showing a Cisco configuration file with the text: `boot-end-marker ! enable secret 5 1Bhsg$izpAqHDUBLzEWCqfP/leT/ enable password 7 0455254C5F765C ! no aaa new-model. system mtu routing 1500 ...`. Another result snippet shows: `enable secret 5 1P6du$.NRbLzz5WIKER5mgw.t7r/ enable password 7 000A3D4C540C1B ! no aaa new-model. system mtu routing 1500. ip subnet-zero ...`. A third result snippet shows: `logging buffered 51200 warnings. enable secret 5 1.7N$Ru28/DDfSHrAgq5bhUFzH enable password 7 151C2546547D25 ! no aaa new-model ! resource ...`. The location "Tempe, AZ" is also visible at the bottom of the search results.



Cloud Docs Exposures

ROBOTS.TXT IS DEAD

Personal photo galleries exposed



Google

Search About 164,000 results (0.33 seconds)

<https://www.dropbox.com/robots.txt>

```
User-agent: *
Disallow: /s/
Disallow: /sh/
Disallow: /static/
Disallow: /gallery/
```

www.dropbox.com/gallery/

[Sommerblut 2011 - Dropbox - Photos - Simplify your life](https://www.dropbox.com/gallery/16453785/1/Sommerblut_2011?...)
https://www.dropbox.com/gallery/16453785/1/Sommerblut_2011?...
 1_COPYRIGHT-HINWEISE 1 image. Last modified 5/18/2011. ADES_18 images. Last modified 5/23/2011. ALFONS_Fotos_wg 12 images .

[GracerHopper112011 - Dropbox - Photos - Simplify your](https://www.dropbox.com/gallery/9183906/.../GracerHopper112011...)
<https://www.dropbox.com/gallery/9183906/.../GracerHopper112011...>
 Dropbox is a free service that lets you bring your photos, docs, and vid share them easily. Never email yourself a file again!



Data Loss In The News

MAJOR DATA LEAKS

- Yale Alumni 43,000 SSNs Exposed in Excel Spreadsheet





NotInMyBackYard



LOCATION, LOCATION, LOCATION

Cloud storage:

- Google Docs, DropBox, Microsoft SkyDrive, Amazon S3

Social networking sites:

- Facebook, Twitter, LinkedIn

Public document sharing sites:

- scribd.com, 4shared.com, issuu.com, docstoc.com,

PasteBin and text sharing sites:

- pastebin.com, pastie.org, ...

Public presentations sharing sites:

- slideshare.net, prezi.com, present.me

Public charts and graphs sharing sites:

- ratemynetworkdiagram.com, gliffy.com, ManyEyes

Video sharing sites:

- vimeo.com, dailymotion.com, metacafe.com, youtube.com



NotInMyBackYard



PASTEBIN EXAMPLE

Where to look

Specific file types to look in

Keywords to add to search that find sensitive information

Found passwords, emails and other personal information

Enter your information to search for across the Internet

John Doe [Remove]
jdoe@gmail.com [Remove]

Search String	Page Title	URL
site:pastebin.com blvd 75th gmai	CC HUGE LIST - Pastebin.com	http://...
site:pastebin.com blvd 75th gmai	AT&TMeetsDigitalCorruption - Pastel	http://pastebin.com/itm460Fj
site:pastebin.com blvd steven gr	email password abhi3chemical@gmail.com	http://pastebin.com/wfuCzYZA
site:pastebin.com blvd steven gr	Chriss1001 Database Leak - Pastebin.com	http://pastebin.com/54wucdR9
site:pastebin.com blvd steven gr	List of Nazis Partisans - Pastebin.com	http://pastebin.com/yu86h9g1
site:pastebin.com blvd steven gr	USA Credit Cards - Fuck US - Pastebin.com	http://pastebin.com/vpSHYjH
site:pastebin.com blvd steven gr	Osiris OwNz Maxprotech - Pastebin.com	http://pastebin.com/e34GUcTy
site:pastebin.com blvd steven gr	paceeducation.ca [Massive Leak] via @Th	http://pastebin.com/zc5mhC0B
site:pastebin.com blvd steven gr	www.ranchomiraoca.gov hacked by i0ke	http://...

Selected Result

```

5 Apr 2012 ... address | city | company | email | fax | fname | id | lname | password | phone | registrationDate |
state | username | zip | ... Ltd. | w.de.inservices@gmail.com | NULL | Pathomphat | 14 ... 13602 WESTLAND
EAST BLVD | HOUSTON | STRESS ... 3365 Silver Ave | Plattsburgh | NULL | toyodakohei@hotmail.com ...

```

NotInMyBackYard

XLS IN CLOUD EXAMPLE

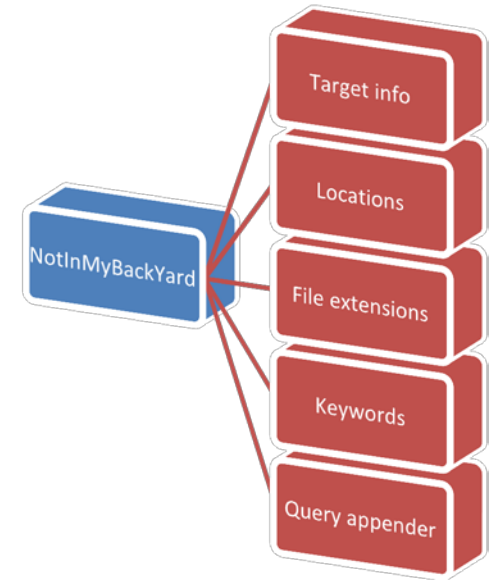


The screenshot shows the NotInMyBackYard tool interface. The search string is 'password'. The search results table is as follows:

Search String	Page Title	URL
site:s3.amazonaws.com ext:xls password	Domains	https://businessmarketing.s3.amazonaws.com/
site:s3.amazonaws.com ext:xls password	Domains	http://media.archonmedia.com.s3.amazonaws.com/
site:s3.amazonaws.com ext:xls password	483685 796337 26 a	http://s3.amazonaws.com/caclubindia/cdn/forum
site:s3.amazonaws.com ext:xls password	here - Amazon Web	http://himis.s3.amazonaws.com/himis-esp.xls
site:s3.amazonaws.com ext:xls password	Support - Amazon S3	https://s3.amazonaws.com/files3.peopleperhour
site:s3.amazonaws.com ext:xls password	september links	https://s3.amazonaws.com/files3.peopleperhour
site:s3.amazonaws.com ext:xls password	Copy_of_user.xls - Ai	http://springpad-user-data.s3.amazonaws.com/2
site:s3.amazonaws.com ext:xls password	Social Networking - A	http://s3-media.s3.amazonaws.com/wp-content/
site:s3.amazonaws.com ext:xls password	Domains	https://internetmarketingwhizkidz.s3.amazonaws.com/

Red callouts highlight specific settings and results:

- "Look for the word 'password'" points to the Query Appender field.
- "Look at Amazon S3 cloud storage uploads" points to the selected location 'site:s3.amazonaws.com'.
- "Look in all Microsoft Excel spreadsheets" points to the selected extension 'ext:xls'.
- "Copy_of_user.xls - Ai" points to a specific search result.



Cloud Docs Exposures

PUBLIC CLOUD SEARCHING

Public cloud storage document exposures



S3 Simple Storage Service

Google search results for the query "password ext:xls site:s3.amazonaws.com". The search shows about 175 results. Two results are highlighted with red boxes:

- Result 1:** [\[XLS\] september links - Amazon S3](#)
URL: <https://s3.amazonaws.com/files3.../Portfolio-224723-sept>
File Format: Microsoft Excel - View as HTML
3, nazikilan@gmail.com, ilangir.net, http://ilangir.net/ilan_c
12-Sep, 18-Sep, 22-Sep, Please enter with username and
- Result 2:** [\[XLS\] Copy of user.xls - Amazon Web Services](#)
URL: springpad-user-data.s3.amazonaws.com/2e.../Copy_of_u
File Format: Microsoft Excel - View as HTML
1, Username, Password, Pin/Notes. 2, MUD, st
Cox, mic...@cox.net, cox... 4, OPP

Finding XLS files with "password" on Amazon S3 cloud storage drives

Username and passwords for bank accounts, email, and everything else

	A	B	C	D
1		Username	Password	Pin/Notes
2	MUD	st...@gmail.com	mu	
3	Cox	mi...@cox.net	cox	
4	OPPD	op...	opp	
5	USAA	ms...	mst	
6	FAFSA		12c	64
7	Metro	mg...	UIC	
8	US Bank	ust...	ust	990
9	Black Hills gas	bla...	bla	
10	phone	mich...	spr	



NEW GOOGLE HACKING TOOLS

Bing Hacking Database v2.0

Bing Hacking Database v2.0

STACH & LIU TOOLS

BHDB v2.0 – Updates

- Bing hacking database
- Bing hacking limitations
 - Disabled **inurl:**, **link:** and **linkdomain:** directives in March 2007
 - No support for **ext:**, **allintitle:**, **allinurl:**
 - Limited **filetype:** functionality
 - Only 12 extensions supported
- **UPDATES (2012)**
 - **ext:** functionality now added
 - **inurl:** work around by using **instreamset:url:**
- New BHDB 2.0
 - Several thousand more Bing dorks!

WEB IMAGES VIDEOS MAPS MORE

bing instreamset:url:"wp-config.php" "define('DB_PASSWORD',' ext:php"

58 RESULTS

Wordpress database passwords in config files

www.matthewtmead.com
www.matthewtmead.com/blog/wp-config.php.b4wpggrade
define('DB_PASSWORD', 'mercury64bio'); // ...and password define('DB_HOST', 'mysql01.discountasp.net'); // 99% chance you won't need to change this value

www.namasteyogaproducts.com
www.namasteyogaproducts.com/magicalbeadstalk/wp-config.php_
define('DB_PASSWORD', 'JD5b7H9X1e'); /** MySQL hostname */ define('DB_HOST', 'localhost'); /** Database Charset to use in creating database tables.

josephlarge.com
josephlarge.com/wp-config.php.back
define('DB_PASSWORD', '_Of8mKiXW'); /** MySQL hostname */ define('DB_HOST', 'localhost'); /** Database Charset to use in creating database tables.

fonearizona.com
fonearizona.com/wp-config.php
define('DB_PASSWORD', '7tZYJFPRJk6D'); /** MySQL hostname */ define('DB_HOST', 'localhost'); /** Database Charset to use in creating database tables.

bing



NEW GOOGLE HACKING TOOLS

BingBinaryMalwareSearch (BBMS)

Bing Malware Search

TARGETING MALWARE

Targeting known malware signatures

The image shows a Bing search interface and a list of malware signatures. The search query is: `filetype:txt "Time Date Stamp: 37fb2583" "Size of Image: 00008000" "Entry Point: 00001020" "Size of Code: 0000a00"`. The search results show a single result from www.terra.es with the following details: **Time Date Stamp: 37fb2583**, **Address of Entry Point: 00001020**, **Base of Code: 00001000**, and **Size of Image: 00008000**. A red callout box points to the search results with the text: **Malware: Trojan.Dropper.Vbs.Dummytag.A**. Above the search interface, a list of malware signatures is shown, with the signature `Trojan.Dropper.Vbs.Dummytag.A:37fb2583:00008000:00001020:0000a00` highlighted in pink.

```
http://www.metasploit.com/research/misc/mwsearch/sigs.txt
```

```
Win32.Netsky.B@mm:4030f459:0001b000:000190d0:00005000
Win32.Sobig.E@mm:3ef89a91:00027000:00025bd6:00000000
Trojan.Muldrop.970:3d4553b8:00008000:00001000:00002400
Trojan.Dropper.Vbs.Dummytag.A:37fb2583:00008000:00001020:0000a00
Win32.Dumar.A@mm:aa3b2cfc:0000b000:00009b40:00002000
```

www.bing.com/search?q=filetype:txt "Time Date Stamp: 37fb2583" "Size of Image: 00008000" "Entry Point: 00001020" "Size of Code: 0000a00"

filetype:txt "Time Date Stamp: 37fb2583" "Size of Image: 00008000" "Entry Point: 00001020" "Size of Code: 0000a00"

Malware:
Trojan.Dropper.Vbs.Dummytag.A

1-1 of 1 results · [Advanced](#)

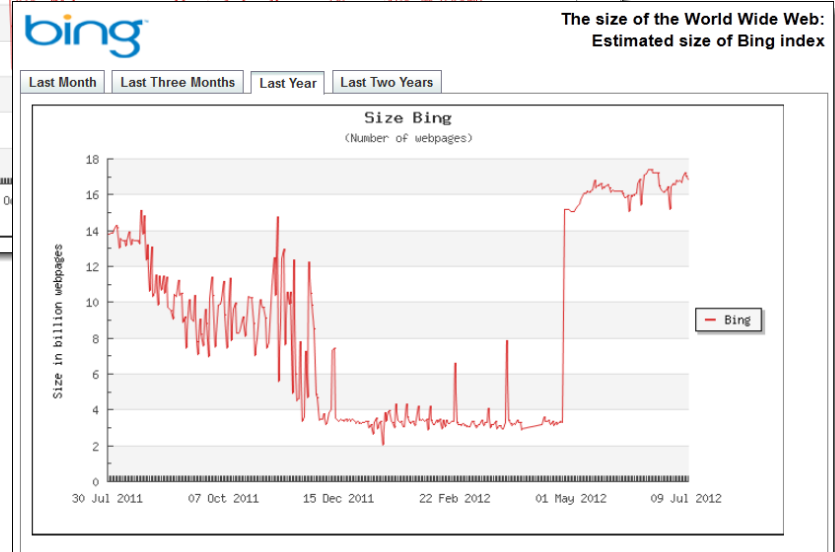
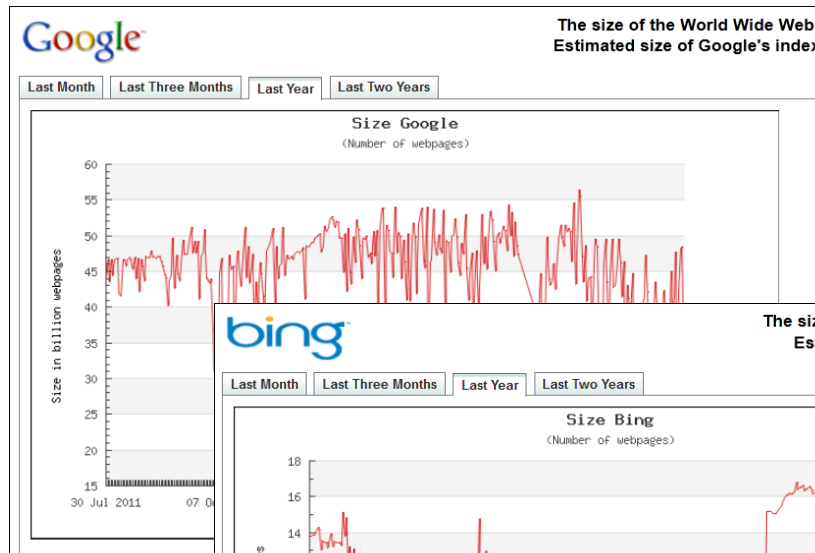
www.terra.es
Time Date Stamp: 37fb2583. Symbols Pointer: 00000000 ... Address of **Entry Point: 00001020**.
Base of Code: 00001000 ... **Size of Image: 00008000**. Size of Headers: 00000400
www.terra.es/personal7/sanchezsignes/PuRSuiT.e_xe

Google vs Bing Size

MORE BANG FOR YOUR SEARCH

Search results

Search engine ↕	Pages indexed ↕
Baidu	?
Bing	3 billion ^[1]
DuckDuckGo	?
Google	50 billion ^[1]
Yahoo!	3.5 billion ^[1]
Yandex	>2 billion ^[4]





NEW GOOGLE HACKING TOOLS

CodeSearch Diggity

Google Code Search



VULNS IN OPEN SOURCE CODE

- Regex search for vulnerabilities in indexed public code, including popular open source code repositories:



- Example: SQL Injection in ASP querystring
 - `select.*from.*request\..QUERYSTRING`

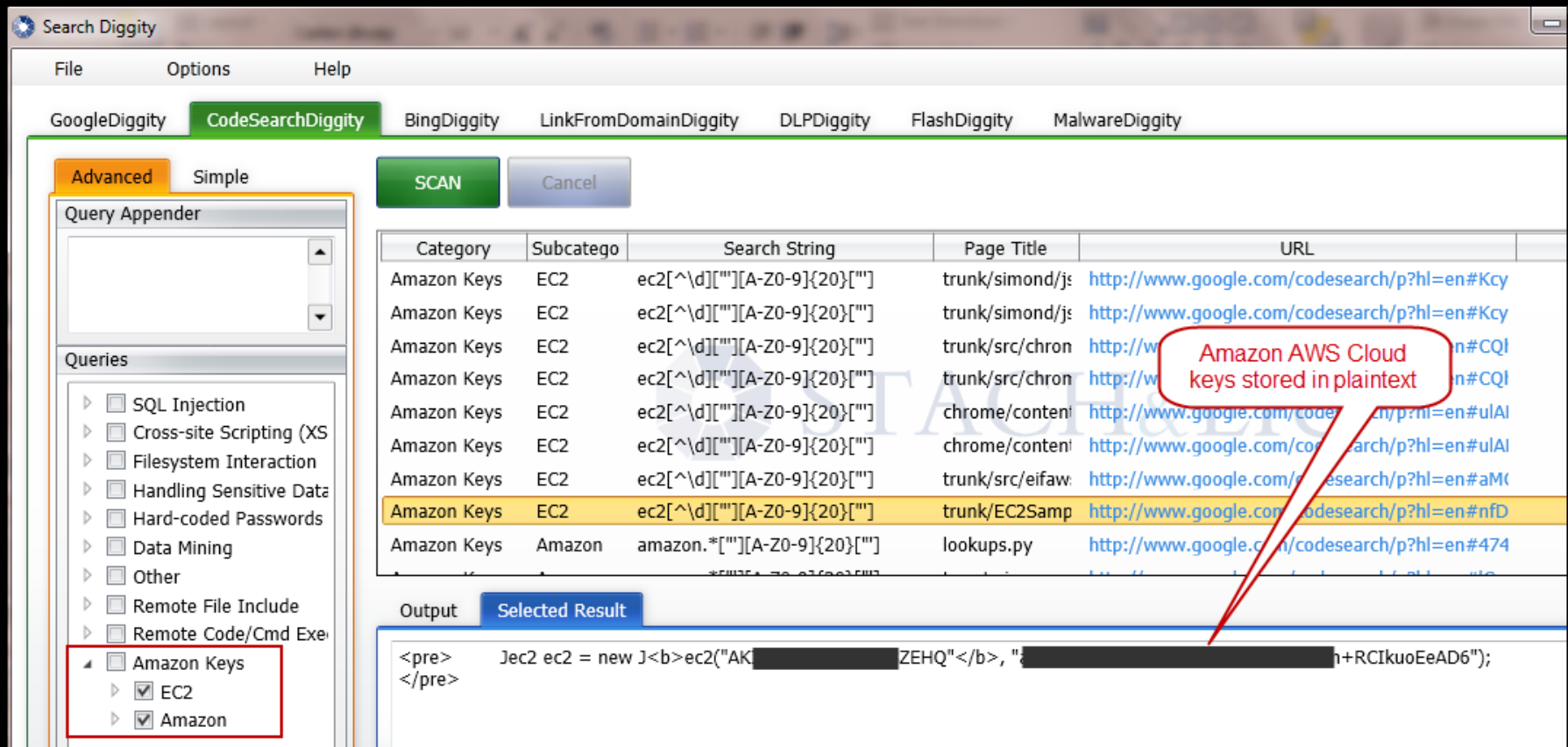
The screenshot shows a Google Code Search result for the query `select.*from.*request\..QUERYSTRING`. The search results list a file named `post.asp`. A red callout box points to the `reply_id` parameter in the SQL query, stating: `reply_id is SQL injectable querystring parameter`. The code snippet shows the following lines:

```
45: strSql = "SELECT * from reply where reply_id = " & Request.QueryString("reply_id")
46: msg = "<br><br>×çÒâ£°Ö»ÓÐ,ÄÏÄÖÄ×÷Öß°Í¹ÙÀìÔ±²ÄÄÛ±à±Öâ,øìû×ó."
57: strSql = "SELECT T Message from Topics where Topic_id = " & Request.QueryString("reply_id")
58: msg = "<br><br>×çÒâ£°Ö»ÓÐ,ÄÏÄÖÄ×÷Öß°Í¹ÙÀìÔ±²ÄÄÛ±à±Öâ,øìû×ó."
```

At the bottom of the search results, there is a link to `www.cnarts.net/eweb/download/software/bbs/tradeforum.zip` with the text "Unknown - ASP - More from tradeforum.zip »".

CodeSearch Diggity

AMAZON CLOUD SECRET KEYS



The screenshot shows the CodeSearch Diggity application window. The 'CodeSearchDiggity' tab is active. On the left, the 'Queries' list has 'Amazon Keys', 'EC2', and 'Amazon' checked. The main table displays search results with columns for Category, Subcategory, Search String, Page Title, and URL. A red callout box points to a result with the URL 'http://www.google.com/codesearch/p?hl=en#nfD', which is highlighted in yellow. Below the table, the 'Selected Result' output shows a code snippet:

```
<pre>
Jec2 ec2 = new J<b>ec2("AK[REDACTED]ZEHQ"</b>, "[REDACTED]+RCIkuoEeAD6");
</pre>
```



Cloud Security

NO PROMISES...NONE

Amazon AWS Customer Agreement

- <http://aws.amazon.com/agreement/#10>

10. Disclaimers.

No guarantee of confidentiality, integrity, or availability (the CIA security triad) of your data in any way

THE SERVICE OFFERINGS ARE PROVIDED "AS IS." WE AND OUR AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICE OFFERINGS OR THE THIRD PARTY CONTENT, INCLUDING ANY WARRANTY THAT THE SERVICE OFFERINGS OR THIRD PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR CONTENT OR THE THIRD PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR AFFILIATES AND LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

Cloud Crawling

CREATE YOUR OWN SEARCH ENGINES



Web Data Extraction

Automate virtually anything you can do with a web browser



Query the World

Tap the web's massive database.

80legs



The most powerful
web-crawler ever.



NEW GOOGLE HACKING TOOLS

SHODAN Diggity

SHODAN



HACKER SEARCH ENGINE

- Indexed service banners for whole Internet for HTTP (Port 80), as well as some FTP (23), SSH (22) and Telnet (21) services

The screenshot shows the SHODAN search interface. The search bar contains the query "Server:NAShttpd". Below the search bar, a table lists the top countries matching the search:

Country	Count
Italy	20
China	14
United States	7
Spain	6
Greece	5

A callout box points to the search results, stating "NAS storage devices located". Below the table, a specific search result is highlighted with a red box. The result details are:

- 123.116.195.215**
- Added on 06.02.2012
- Beijing

The service banner for this IP is displayed below the IP address:

```
HTTP/1.0 401 Unauthorized
Server: NAShttpd
Date: Mon, 06 Feb 2012 18:01:34 GMT
WWW-Authenticate: Basic realm="Default USER:admin"
Content-Type: text/html
Connection: close
```

A callout box points to the "WWW-Authenticate" header, stating "Default username is 'admin'".

SHODAN



FINDING SCADA SYSTEMS

The screenshot shows the SHODAN search interface with the search term 'scada' entered in the search bar. A red callout box points to the search bar with the text 'Using SHODAN to find SCADA web admin interfaces'. Below the search bar, there is a table of top countries matching the search:

Country	Count
Canada	13
Finland	12
United States	8
Sweden	6
Denmark	6

Below the table, two search results are shown. The first result is for IP address **218.111.69.68**, added on 11.06.2011, located in Kuala Lumpur. The second result is for IP address **66.18.233.232**, added on 20.04.2011, located in Calgary. Both results show HTTP/1.0 401 Authorization Required status and WWW-Authenticate headers. The first result's WWW-Authenticate header is 'Basic realm="iSCADA Gateway User Login"', which is highlighted with a red box. The second result's WWW-Authenticate header is 'Digest realm="RTS SCADA Server", nonce="Z9PJNF+hB'.

SHODAN Diggity



FINDING SCADA SYSTEMS

The screenshot shows the SHODAN Diggity interface. The 'Shodan' tab is selected. The 'Settings' panel shows the 'API Key' field, which is highlighted with a red box and a callout 'Enter SHODAN API key'. The search results table is as follows:

Category	Search String	URL	Hostnames	City	Country
SCADA	Niagara Web Server	http://193.185.169.90/			Finland
SCADA	Niagara Web Server	http://12.171.57.87/			United States
SCADA	Niagara Web Server	http://70.168.40.243/	wsip-70-168-40-243.	Cleveland	United States
SCADA	Niagara Web Server	http://216.241.207.94/	sciop-ip94.scinternet.	Colorado City	United States
SCADA	Niagara Web Server	http://206.82.16.227/	niagarafred.norleb.ki	Lancaster	United States
SCADA	Niagara Web Server	http://184.187.11.158/		Omaha	United States

The 'Output' panel shows the selected result for the URL <http://70.168.40.243/>, with a callout 'Finding SCADA systems via SHODAN Diggity'. The output text is:

```
HTTP/1.0 302 Moved Temporarily
location: http://70.168.40.243/login
content-type: text/html; charset=UTF-8
content-length: 116
set-cookie: niagara_audit=guest; path=/
server: Niagara Web Server/3.5.34
```


Advanced Defenses

PROTECT YO NECK

Diggity Alert DB

DATA MINING VULNS



Database Browser

File View Connections Execute Help

Connections: 0001 select AlertTable.* from AlertTable
0002

AlertDB

Tables: AlertTable

Drag a column header here to group by that column

PubDate	DateGRShared2	Title	URLClean
2011-07-31T00:23:07Z	Sat Jul 30 17:23:07 2011	PHP Tutorials: Form Data Display and Sec	http://blog.phpmoz.org/php-tutor
2011-07-30T23:41:34Z	Sat Jul 30 16:41:34 2011	error_log	http://celestedesignsusa.com/err
2011-07-30T23:41:34Z	Sat Jul 30 16:41:34 2011	RC Plane » Nine eagles Kategori: Nine eagles View:	http://depok-aeromodelling.com/c

0001 select AlertTable.* from AlertTable
0002

Drag a column header here to group by that column

PubDate	DateGRShared2	Title	URLClean	DiggityFeedSource
2011-07-31T00:23:07Z	Sat Jul 30 17:23:07 2011	PHP Tutorials: Form Data Display and Sec	http://blog.phpmoz.org/php-tutorials-form-data-display-and-security	Google Alerts - data filety
2011-07-30T23:41:34Z	Sat Jul 30 16:41:34 2011	error_log	http://celestedesignsusa.com/error_log	Google Alerts - "Warning:
2011-07-30T23:41:34Z	Sat Jul 30 16:41:34 2011	RC Plane » Nine eagles Kategori: Nine eagles View:	http://depok-aeromodelling.com/category/295/nine-eagles	Google Alerts - "Warning:
2011-07-31T00:01:58Z	Sat Jul 30 17:01:58 2011	Eliza Dushku Central / Photo Gallery	http://eliza-dushku.org/gallery/displayimage.php?album=1020&pid=6	Google Alerts - "Powered

Future Directions

WHAT WILL HAPPEN

Diggity Dashboards

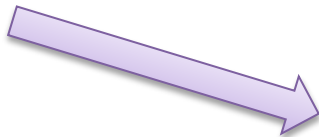
COMING SOON



DIGGITY ALERTS
CLOUD DATABASE



Google Charts



Mobile BI Apps

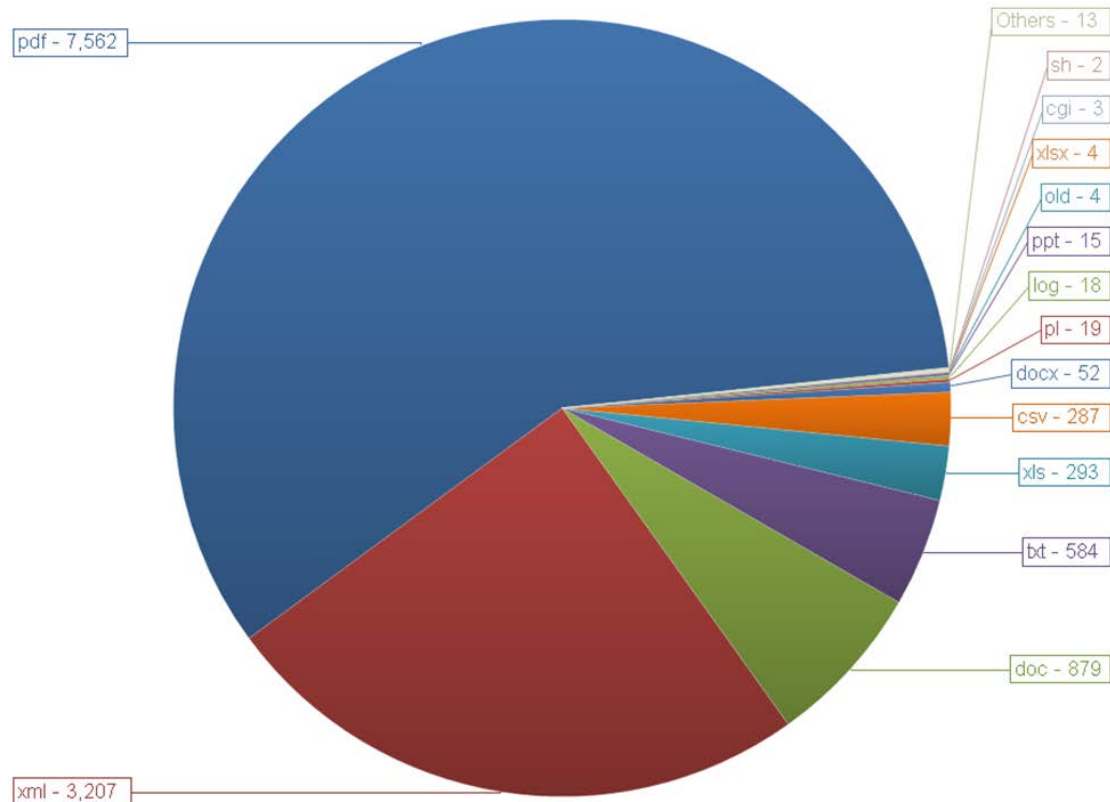


DLP Reporting

PRACTICAL EXAMPLES

DLPDiggity - # of Files Analyzed per File Extension

Total = 12,943 files





Questions?
Ask us something
We'll try to answer it.

For more info:
Fran Brown
Rob Ragan (@sweepthatleg)
Email: contact@stachliu.com
Project: diggity@stachliu.com
Stach & Liu, LLC
www.stachliu.com



Thank You

Stach & Liu Google Hacking Diggity Project info:

<http://www.stachliu.com/index.php/resources/tools/google-hacking-diggity-project/>