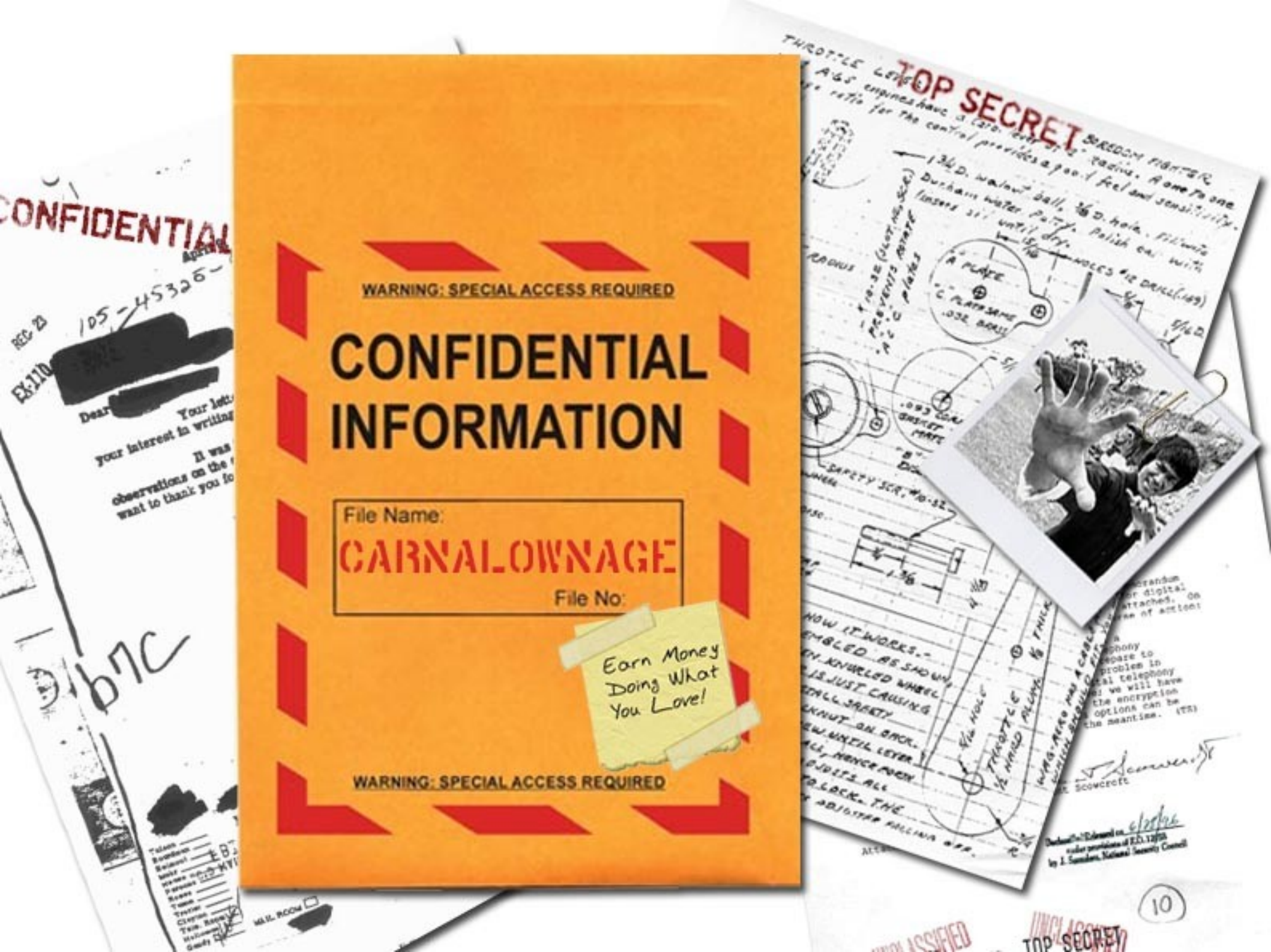
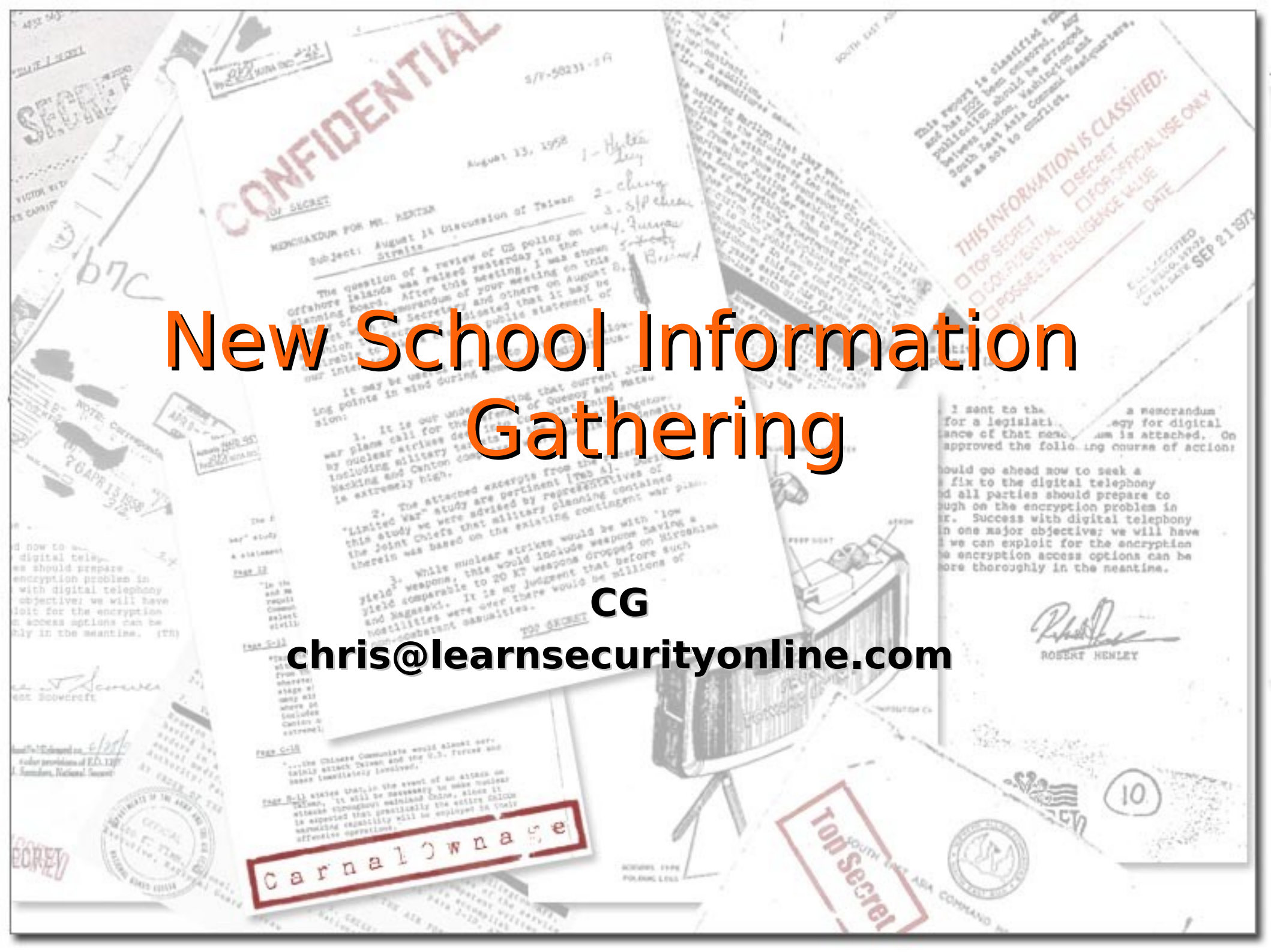

WARNING: SPECIAL ACCESS REQUIRED
CONFIDENTIAL
INFORMATION
File Name:
CARNALOWNAGE
File No:
Earn Money Doing What You Love!
WARNING: SPECIAL ACCESS REQUIRED
TOP SECRET
CONFIDENTIAL
UNCLASSIFIED
TOP SECRET



New School Information Gathering

CG

chris@learnsecurityonline.com

Who Am I?

- Penetration Tester for Northrop Grumman
- EthicalHacker.net columnist
- LearnSecurityOnline.com

Agenda

- New School?
- Open Source Intelligence Gathering (OSINT)
- FierceDNS
- SEAT/Goolag
- Google Mail Harvesters
- Metagoofil
- Online Tools
  - Netcraft/ServerSniff/DomainTools/CentralOps/Clez.net/Robtex
- Maltego

New School?

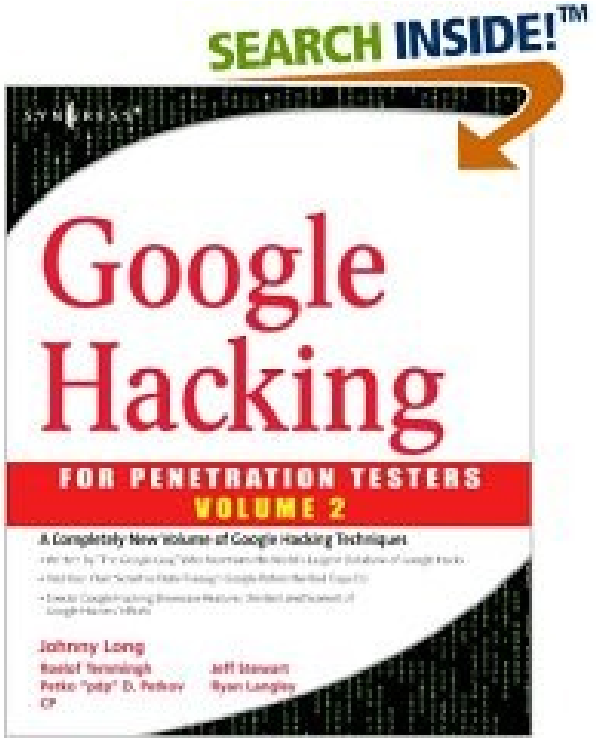
- New School, just a “new” way of looking at Information Gathering, less just discovering network blocks (whois) and more take a “full spectrum” look at your target.
- OSINT, Open Source Intelligence
  - Out on the net for everyone to find, if you know what to look for
  - Domain Names
  - Files containing useful information
  - Email addresses
  - Website Source
  - Etc (we’ll get into the etc)

OSINT

- Generally no direct contact with victim's servers OR no non-standard traffic directed toward victim
- End Result?
  - Organization's net blocks, external servers IPs and domain names, internal IP ranges, emails to send phishing attacks to, phone numbers to call, trust relationships with other organizations, & other relevant information for your audit and hopefully identifying exploitable flaws in the target's network

Isn't that what Google is for?

- Yeah kinda, Google-fu is important but we're not going to talk much about Google hacking, go read the book.



OSINT

- Information Gathering & Domain Name Search
  - Whois info, NS & AS Reports
  - Search using target domain name
    - Target.com
  - and subdomain name
    - Vulnerable.target.com
  - Who's handling mail, DNS, net blocks, web hosting, etc

OSINT

- Information Gathering & Key Words
- Use that google-fu!
  - Password
  - Login
  - Target specific key words
  - Database/Secret/yak yak
  - Google dorks
  - Use SEAT/Goolag to audit a specific domain

OSINT

- Information Gathering & File Search
- Looking for
  - Network diagrams (.vsd, .jpg, .gif)
  - Databases (.mdb)
  - Papers & documents (.doc, .pdf, .sdw)
  - Presentations (.ppt, .odp)
  - Spreadsheets (.xls, .ods, .sdc)
  - Configuration files (.txt, .rft)
- Thanks metagoofil!

OSINT

- Information Gathering & Email addresses
  - Harvesting scripts
- Information Gathering & Cached Data/Links
  - Archive.org, waybackmachine, Google
- Information Gathering & Source Code
  - Spider the site, look at html source and comments, file paths, file names, scripts used on the site

Tools of the Trade

Some, not all, plenty of others

Tools grouped by category and less by an actual order of doing things or methodology

Fierce DNS

- http://ha.ckers.org/fierce/
- By Rsnake from ha.ckers.org
- “It is meant specifically to locate likely targets both inside and outside a corporate network.”

Fierce DNS

- First it queries your DNS for the DNS servers of the target. It then switches to using the target's DNS server.
- Fierce then attempts to dump the SOA records for the domain in the very slim hope that the DNS server that your target uses may be misconfigured (attempts a zone transfer).*
- Once that fails (because it almost always will) it attempts to "guess" names that are common amongst a lot of different companies (hosts file).

Fierce DNS

- Next, if it finds anything on any IP address it will scan up and down a set amount looking for anything else with the same domain name in it using reverse lookups .
- If it finds anything on any of those it will recursively scan until it doesn't find any more.

Fierce DNS

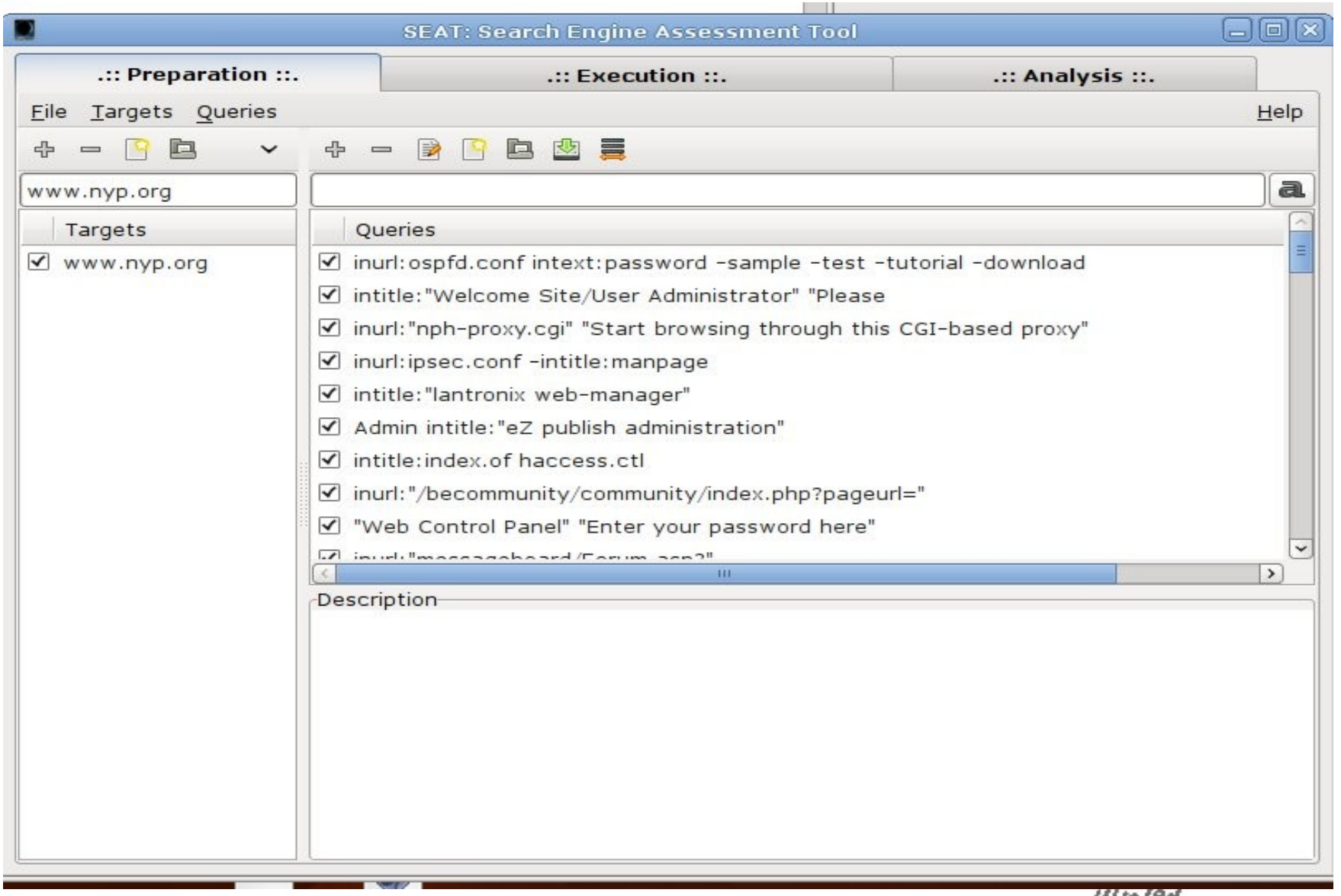
- Examples…

Search Engine Tools

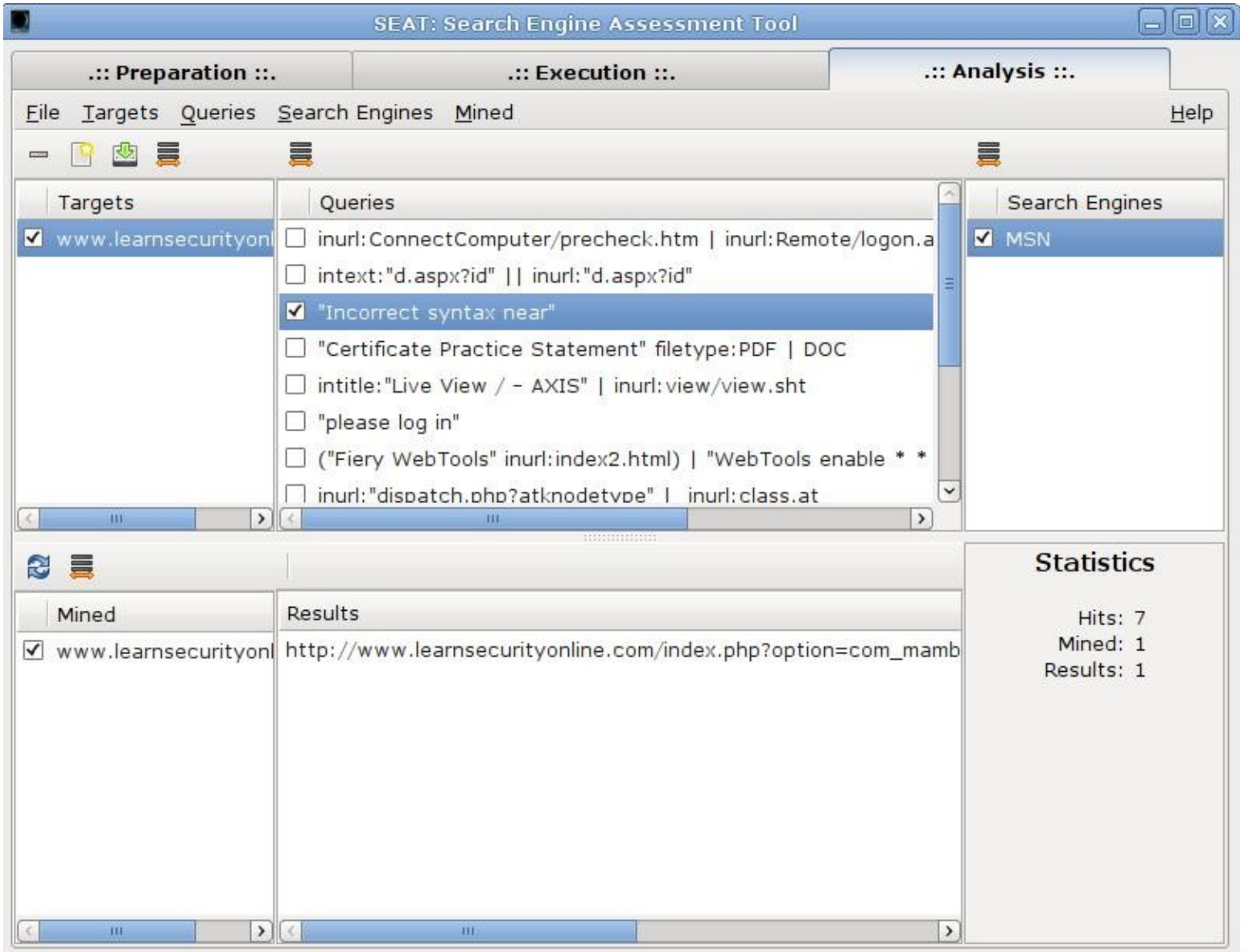
SEAT (Search Engine Assessment Tool)

- By Midnight Research Labs
- http://midnightresearch.com/projects/search-engine-assessment-tool/
- “SEAT uses information stored in search engine databases, cache repositories, and other public resources to scan a site for potential vulnerabilities. It’s multi-threaded, multi-database, and multi-search-engine capabilities permit easy navigation through vast amounts of information with a goal of system security assessment.”
- Think automated GHDB on steriods ☺

SEAT (Search Engine Assessment Tool)



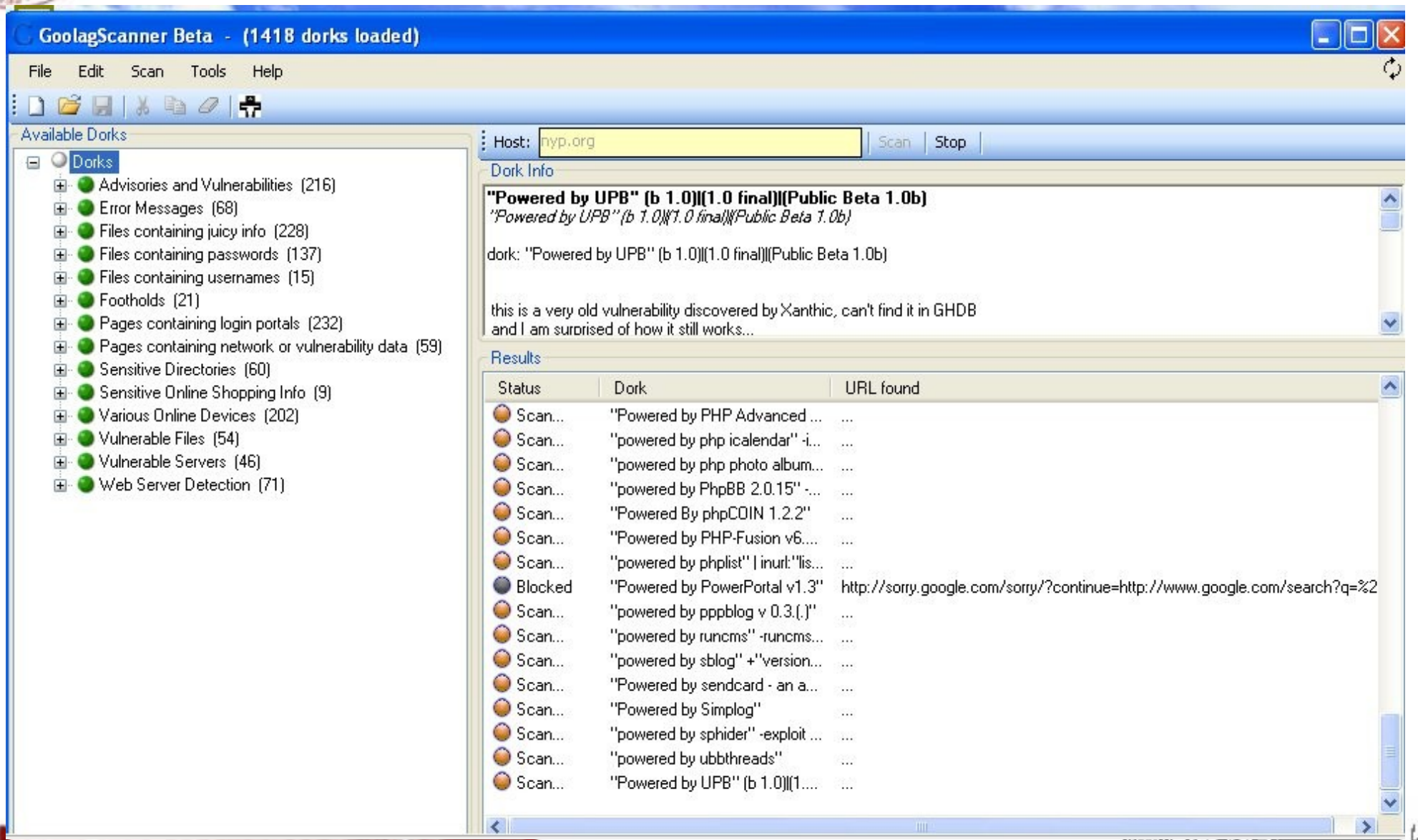
SEAT (Search Engine Assessment Tool)



Goolag

- Cult of Dead Cow's Goolag
- http://www.goolag.org/download.html

Goolag



Email Harvesting

Google Mail Harvesters

- Goog-mail.py
- theHarvester.py
- There are plenty out there
- ***ensure you modify scripts if the victim has a location(s) outside of US to use the appropriate google; google.de. google.be, etc
- may want to change the regex to search for different things [at] <at> (at)

Google Mail Harvesters

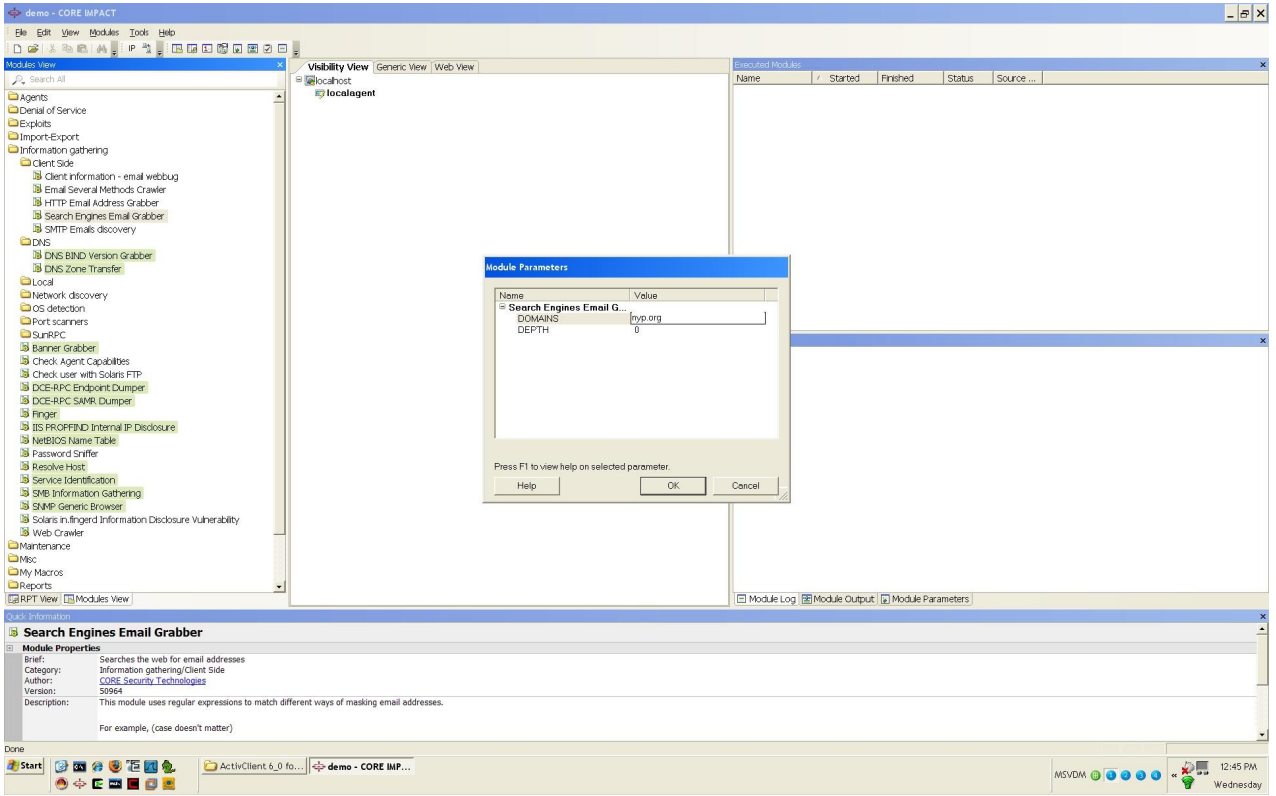
- Goog-mail.py

Google Mail Harvesters

- theHarvester.py
- http://www.edge-security.com/theHarvester.php

Using CORE IMPACT for Email Harvesting

- I'm not a CORE salesman…but if you already have it in your shop…the email harvesting isn't too bad.



Using CORE IMPACT for Email Harvesting

- Different levels of depth
  - Level 0 takes a couple of minutes
  - Level 1 takes a couple of hours
  - Level 2 takes a couple of days
- Can immediately send your client side attacks with those emails in CORE ☺

Document Metadata Extraction

Metagoofil

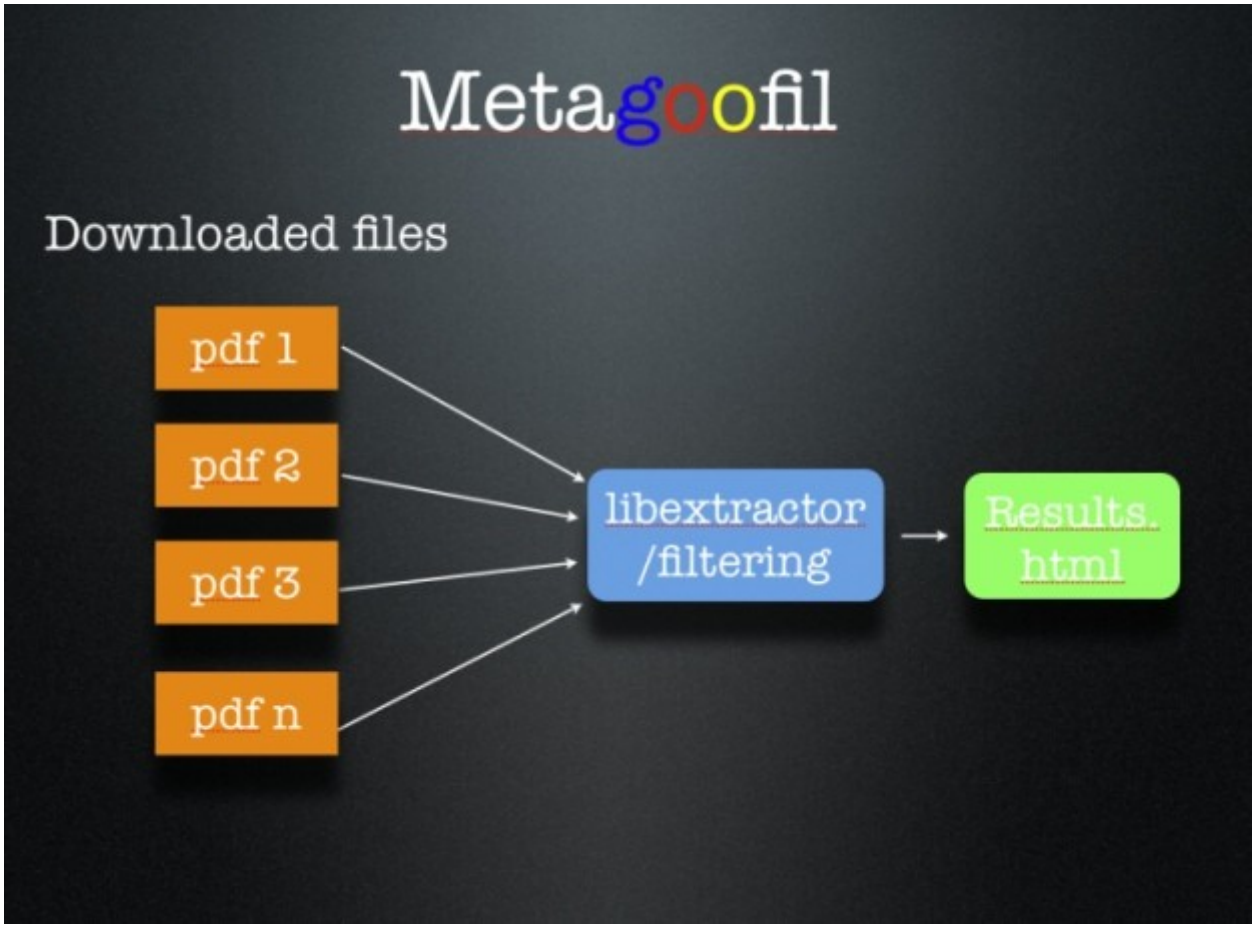
- Meta-what???
- MetaGoofil - Metadata analyzer, information gathering tool.

  http://www.edge-security.com/metagoofil.php
- “Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,odp,ods) available in the target/victim websites.

Metagoofil

- “It will generate a html page with the results of the metadata extracted, plus a list of potential usernames and path disclosure, can be useful for preparing a bruteforce attack on open services like ftp, pop3,web applications, vpn, etc.”

Metagoofil



Metagoofil

```
mimetype - application/msword
revision history - Revision #1: Author 'Manny [redacted]' worked on ''
revision history - Revision #0: Author 'Charles [redacted]' worked on ''
language - U.S. English
paragraph count - 45
line count - 162
last saved by - Manny [redacted]
character count - 19525
template - Normal.dot
creation date - 2002-08-30T03:12:00Z
title - VIII
word count - 3425
page count - 1
creator - Charles [redacted]
date - 2002-09-04T07:12:00Z
generator - Microsoft Word 10.0
```

Total results for doc: 3

Searching in nyp.org for: ppt files.

Total available files: 2
http://www.nyp.org/MungoBlobs/998/594/Heart_Healthy_Basics.ppt

Local copy Open

Important metadata:

```
mimetype - application/vnd.ms-powerpoint
paragraph count - 39
last saved by - Lisa [redacted]
template - Slit
creation date - 2006-01-05T01:14:12Z
title - Heart Healthy Basics
```

Carnal Ownage

11/10/94
Classified by [redacted] b7C
Declassify on: OADR
CA# 94-1720 CRR

Why Metadata?

- Metadata can:
- Reveal the creator of a document, and even a possible network username or derive naming convention.
- Reveal the application that created the document.
- Reveal the **version** of the software that created the document.
- Reveal creation date. Document was created recently with vulnerable version.
- So, now we have a possible username, application used by that individual and the software version. Now we can deliver a directed client side attack for something installed in the enterprise.

On-line Tools

Netcraft

- http://uptime.netcraft.com/
- Netcraft can tell you what OS the web server is running and domain information for the site but it can also show uptime for some sites. This can be useful to see if a site was taken down or rebooted to apply a patch.
- The bummer is most sites are not being monitored and they can't monitor some operating systems like OSX.

Netcraft

Whats that site running? zerodaysolutions.com Search

OS, Web Server and Hosting History for zerodaysolutions.com

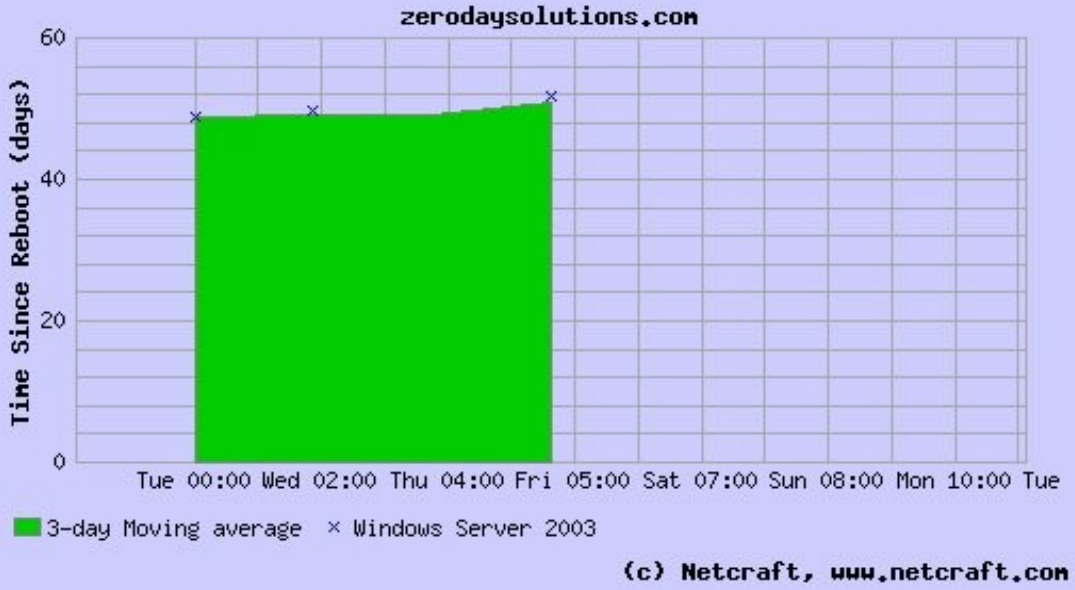
http://zerodaysolutions.com was running Microsoft-IIS on Windows Server 2003 when last queried at 3-May-2008 08:46:50 GMT - refresh now Site Report FAQ
Try out the Netcraft Toolbar!

OS	Server	Last changed	IP address	Netblock Owner
Windows Server 2003	Microsoft-IIS/6.0	27-Apr-2008	198.173.76.252	NTT America, Inc.

Samples of system uptime at zerodaysolutions.com

Note: Uptime - the time since last reboot is explained in the FAQ

Latest data
2-May-2008



Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR
CA# 94-1720 CRR

ServerSniff.net

- http://serversniff.net/
- NS Reports

Carnal Ownage

ServerSniff.net

- AS Reports

ServerSniff.net

- Subdomains

Carnal Ownage

11/10/94
Classified by [redacted] b7C
Declassify on: OADR
CA# 94-1720 CRR

ServerSniff.net

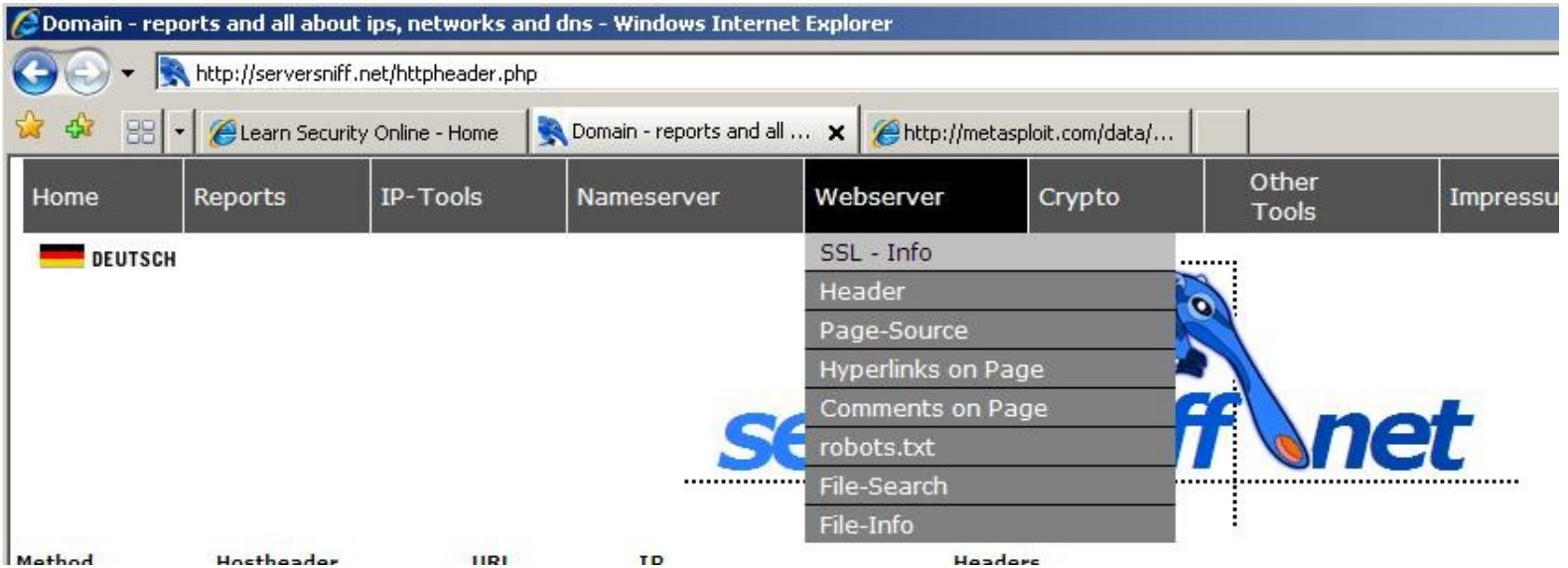
- Hostnames on an IP

ServerSniff.net

- Hostnames on a DNS server

ServerSniff.net

- Web Tools



ServerSniff.net

- Web Tools (Show hyperlinks in a page)

ServerSniff.net

- Web Tools (Show comments in HTML)

ServerSniff.net

- Web Tools (Show HTML Source)

ServerSniff.net

- Web Tools (web server headers)

ServerSniff.net

- Web Tools (SSL information)

DomainTools.com

- http://www.domaintools.com/

DomainTools.com

- How many domain are hosted on EthicalHacker.net's IP address?

DomainTools.com

- Hosting history for EH.net

DomainTools

DomainTools Live Auction starts closing in about...
4 days 58 mins 36 secs

Welcome CG_ | Logout | My Account

Whois | Domain Suggestions | For Sale | Auctions | Advanced Auctions | Domain Search | Domain Monitor

Domain Directory | Ping | Traceroute | My IP Address | Domain Parking Beta | Cheap Domain Name Registration | Bulk Check | Domain Typo Generator | more >

Power Tools: Reverse IP | Domain History | Mark Alert | Name Server Spy | Hosting History | Registrant Search | Registrant Alert new | Forum new

Hosting History for Ethicalhacker.net

Domain Search

Enter a Domain Name

Domain Name: ethicalhacker.net Get History

Enter a domain name into the search box to retrieve the hosting history.

IP Address History

Event Date	Action	Pre-Action IP	Post-Action IP
2004-08-14	Not Resolvable	63.251.163.115	-none-
2004-09-29	New	-none-	217.160.226.73
2005-06-11	Change	217.160.226.73	82.165.199.10
2005-06-18	Change	82.165.199.10	82.165.129.30
2006-01-15	Change	82.165.129.30	82.165.170.112
2006-04-02	Change	82.165.170.112	82.165.178.72
2006-04-15	Change	82.165.178.72	82.165.177.220
2007-05-13	Change	82.165.177.220	74.208.46.66

Note: The current IP location and IP whois may not be the same as it was on the event date.

Registrar History

Date	Registrar
2003-06-28	eNom.com
2004-09-27	Schlund.de

Name Server History

Event Date	Action	Pre-Action Server	Post-Action Server
2002-04-30	Delete	Trivalent.net	-none-
2002-05-02	New	-none-	Trivalent.net
2002-06-28	Transfer	Trivalent.net	Afternic.com
2003-04-30	Delete	Afternic.com	-none-
2003-06-30	New	-none-	Name-services.com
2004-08-10	Delete	Name-services.com	-none-
2004-09-29	New	-none-	1and1.com

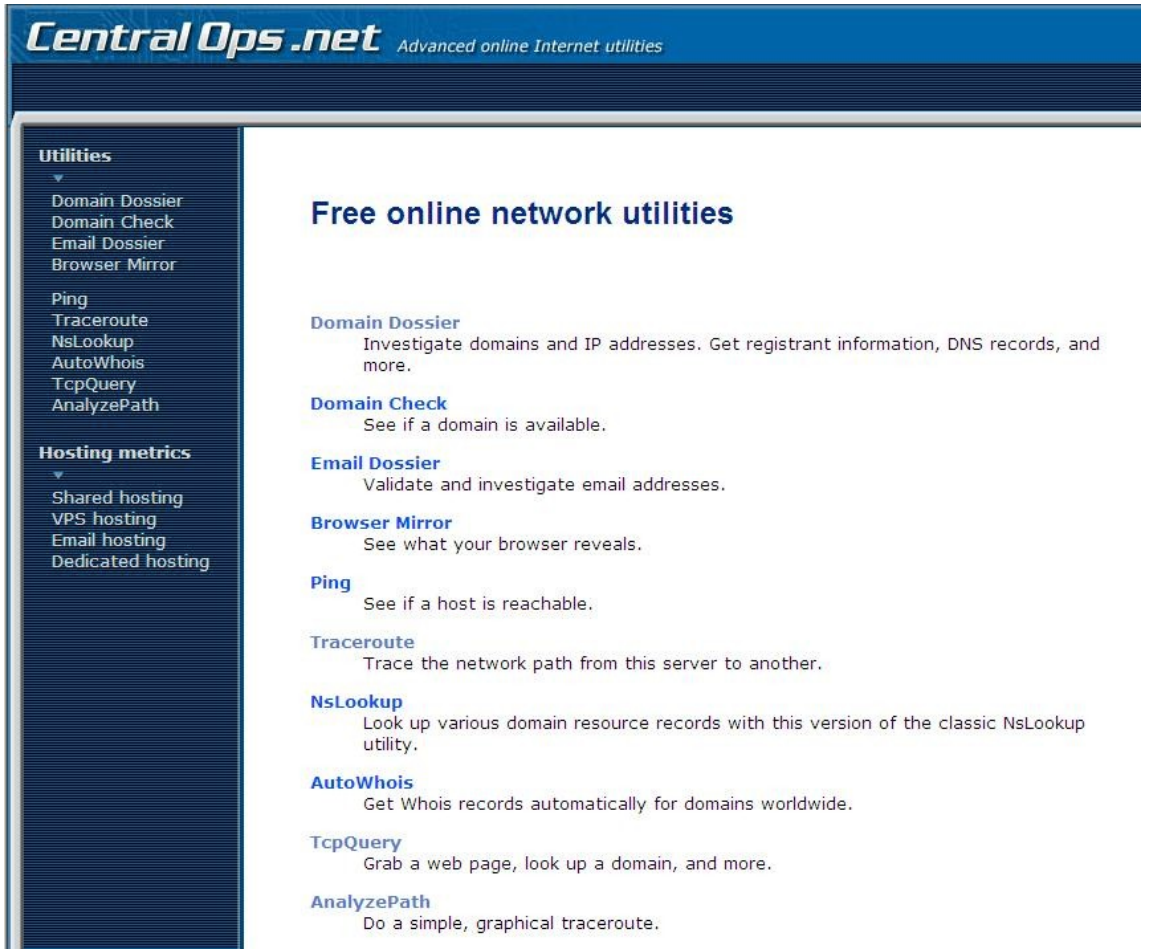
```
C:\WINNT\system32\cmd.exe
Z:\>ping www.ethicalhacker.net
Pinging www.ethicalhacker.net [74.208.46.66] with 32 bytes of data:
```

Carnal Ownage

11/10/94
Classified by [redacted] b7C
Declassify on: OADR
CA# 94-1720 CRR

CentralOps.net

- http://centralops.net/co/



CentralOps.net

- TCP Queries

CentralOps.net

- Traceroute

Carnal Ownage

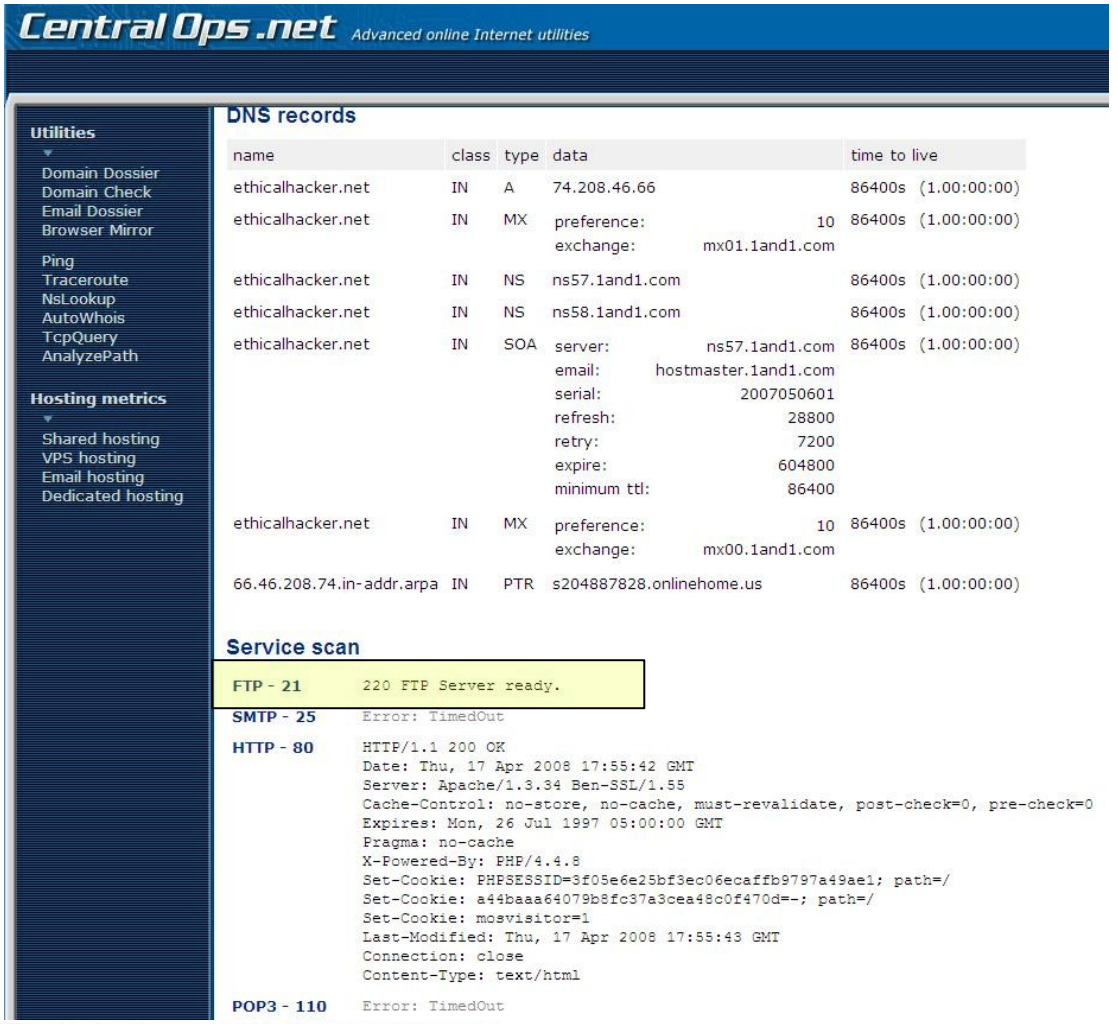
11/10/94
Classified by [redacted] b7C
Declassify on: OADR
CA# 94-1720 CRR

CentralOps.net

- Whois information

CentralOps.net

- DNS information and Service Scans (example 2)



CentralOps.net Advanced online Internet utilities

Utilities
- Domain Dossier
- Domain Check
- Email Dossier
- Browser Mirror
- Ping
- Traceroute
- NsLookup
- AutoWhois
- TcpQuery
- AnalyzePath

Hosting metrics
- Shared hosting
- VPS hosting
- Email hosting
- Dedicated hosting

DNS records

name	class	type	data	time to live
ethicalhacker.net	IN	A	74.208.46.66	86400s (1.00:00:00)
ethicalhacker.net	IN	MX	preference: 10 exchange: mx01.1and1.com	86400s (1.00:00:00)
ethicalhacker.net	IN	NS	ns57.1and1.com	86400s (1.00:00:00)
ethicalhacker.net	IN	NS	ns58.1and1.com	86400s (1.00:00:00)
ethicalhacker.net	IN	SOA	server: ns57.1and1.com email: hostmaster.1and1.com serial: 2007050601 refresh: 28800 retry: 7200 expire: 604800 minimum ttl: 86400	86400s (1.00:00:00)
ethicalhacker.net	IN	MX	preference: 10 exchange: mx00.1and1.com	86400s (1.00:00:00)
66.46.208.74.in-addr.arpa	IN	PTR	s204887828.onlinehome.us	86400s (1.00:00:00)

Service scan

FTP - 21
```
220 FTP Server ready.
```
SMTP - 25
```
Error: TimedOut
```
HTTP - 80
```
HTTP/1.1 200 OK
Date: Thu, 17 Apr 2008 17:55:42 GMT
Server: Apache/1.3.34 Ben-SSL/1.55
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Pragma: no-cache
X-Powered-By: PHP/4.4.8
Set-Cookie: PHPSESSID=3f05e6e25bf3ec06ecaffb9797a49ae1; path=/
Set-Cookie: a44baaa64079b8fc37a3cea48c0f470d=-; path=/
Set-Cookie: mosvisitor=1
Last-Modified: Thu, 17 Apr 2008 17:55:43 GMT
Connection: close
Content-Type: text/html
```
POP3 - 110
```
Error: TimedOut
```

CentralOps.net

- Email Verification (failure)

CentralOps.net

- Email Verification (success)

Clez.net

- Query port and service information

Clez.net

- Query port and service information

net.app
what's up and running?

idn www.learnsecurityonline.com : 80 go Net Head protocol hint http

info | scan result | port list (27)

HTTP HEAD Request

HTTP/1.1 200 OK	
Date	Tue, 22 Apr 2008 01:06:34 GMT
Server	Apache/2.0.54 (Fedora)
X-Powered-By	PHP/5.0.4
Set-Cookie	PHPSESSID=at0g12f2ml8hgam74cf80bdcs3; path=/
Expires	Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control	no-store, no-cache, must-revalidate
Pragma	no-cache
Set-Cookie	b9b2496ce58424ac21fc8aa21ea95431=39f1b88a14b54b4957
eaaba4e05c695b; expires=Tue, 22 Apr 2008 13	06:34 GMT; path=/
Set-Cookie	mosvisitor=1
Last-Modified	Tue, 22 Apr 2008 01:06:35 GMT
Cache-Control	post-check=0, pre-check=0
Connection	close
Content-Type	text/html; charset=UTF-8

Elapsed time: **1.678** seconds.

Clez.net

- Query port and service information

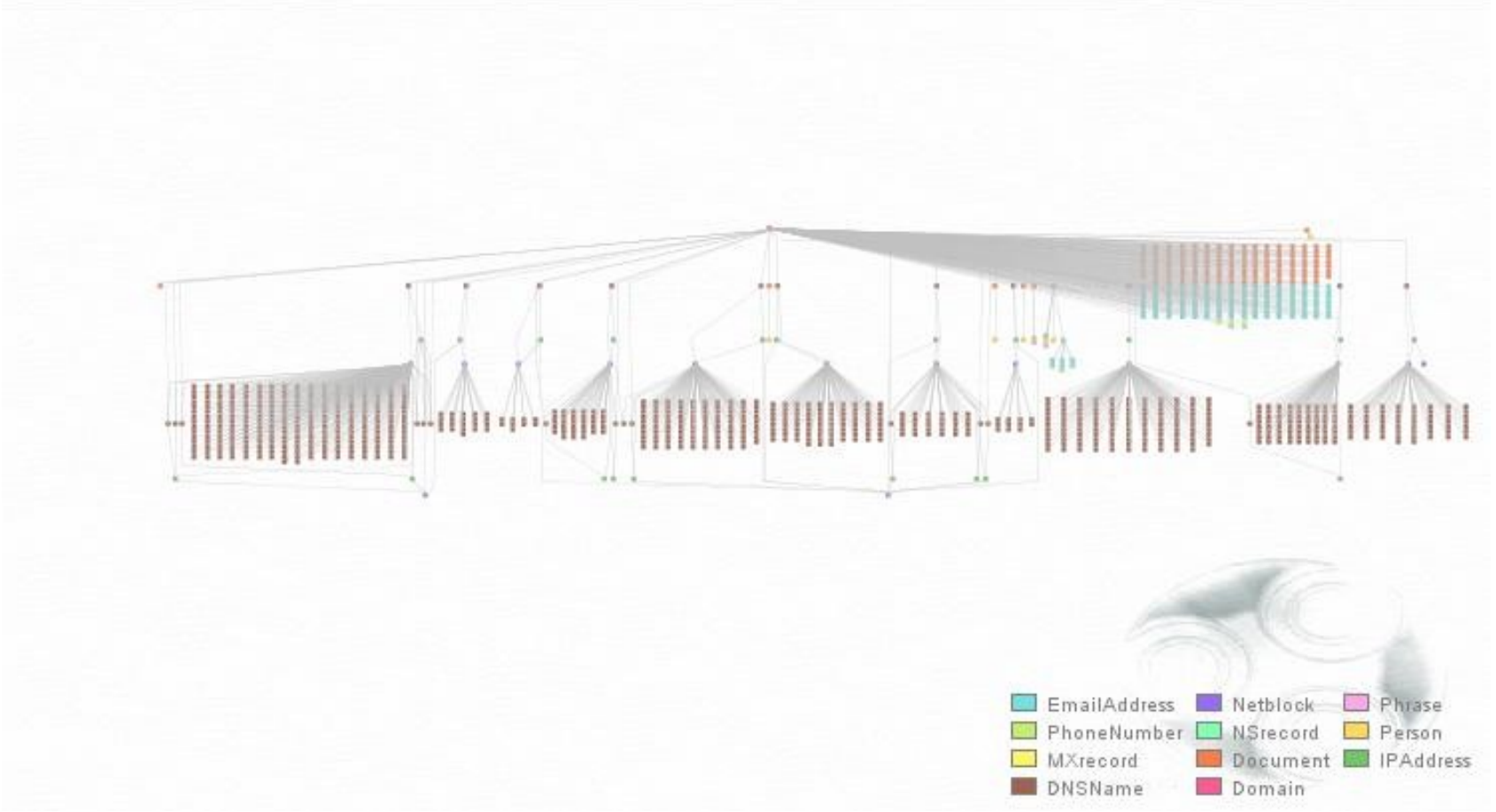
Robtex

- http://www.robtex.com/ Similar to ServerSniff
- Predates ServerSniff, use if ServerSniff is down

Tying it all together with Maltego

Maltego

- What does this tell me about our target domain?

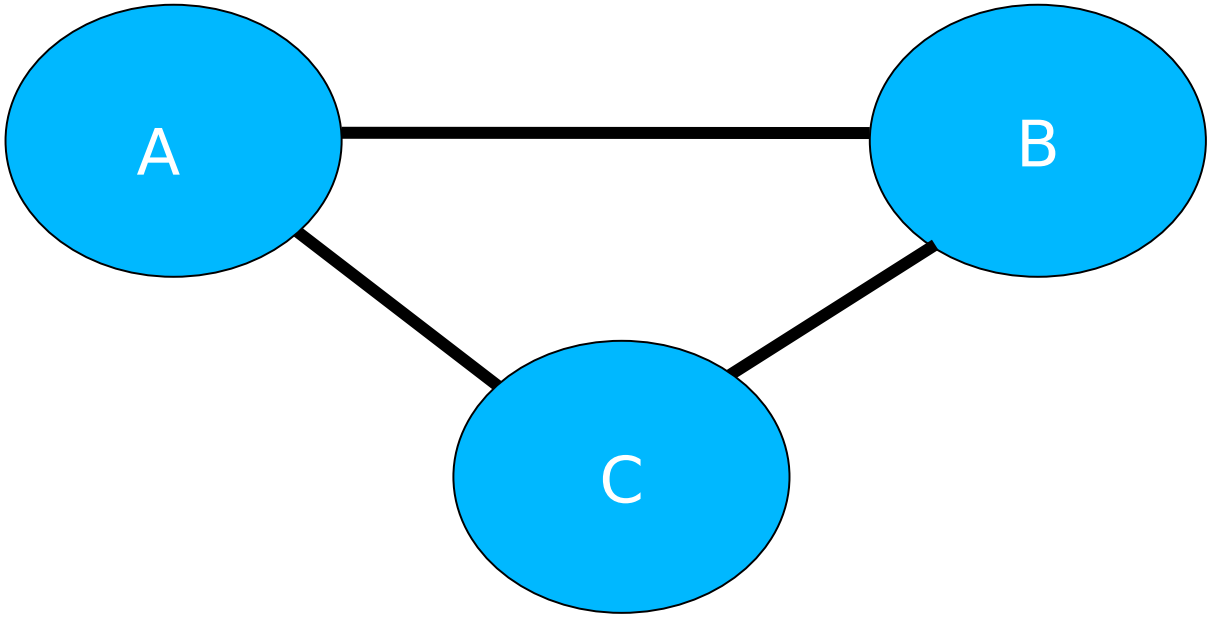


Maltego

- http://www.paterva.com/web2/Maltego/maltego.html
- By Roelof Temmingh from Paterva
- **What is it?**
- Maltego is a program that can be used to determine the relationships and real world links between:
  - People
  - Groups of people (social networks)
  - Companies
  - Organizations
  - Web sites
  - Internet infrastructure such as:
    - Domains
    - DNS names
    - Netblocks
    - IP addresses
  - Phrases
  - Affiliations
  - Documents and files
- All using open source intelligence (OSINT)

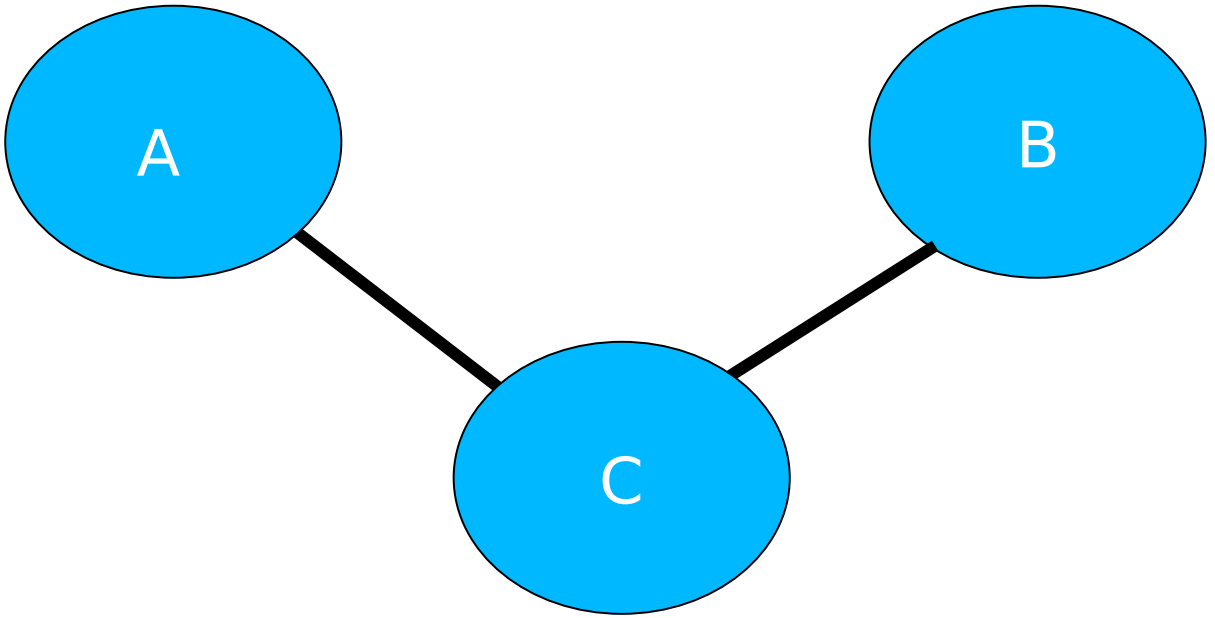
Maltego

- Basically…
- We know A is related to B but they are both related to C, or…



Maltego

- We can see that A and B are related **through** C



Maltego

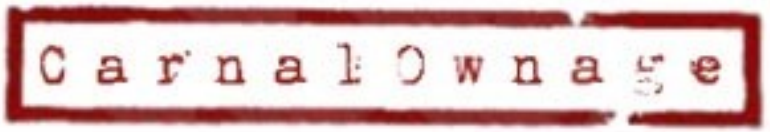
- Find our MX and NS servers

Maltego

- See what hostnames are shared by the DNS servers

Maltego

- Brute force our domain names and resolve them to IPs



Maltego

- Turn each of those IPs into netblocks and do DNS lookups for each class C, you can also resolve those to IPs.

Maltego

- Harvest emails for the domain and verify them.

Maltego

- Harvest documents for the domain and parse the metadata, get emails and usernames.

Maltego

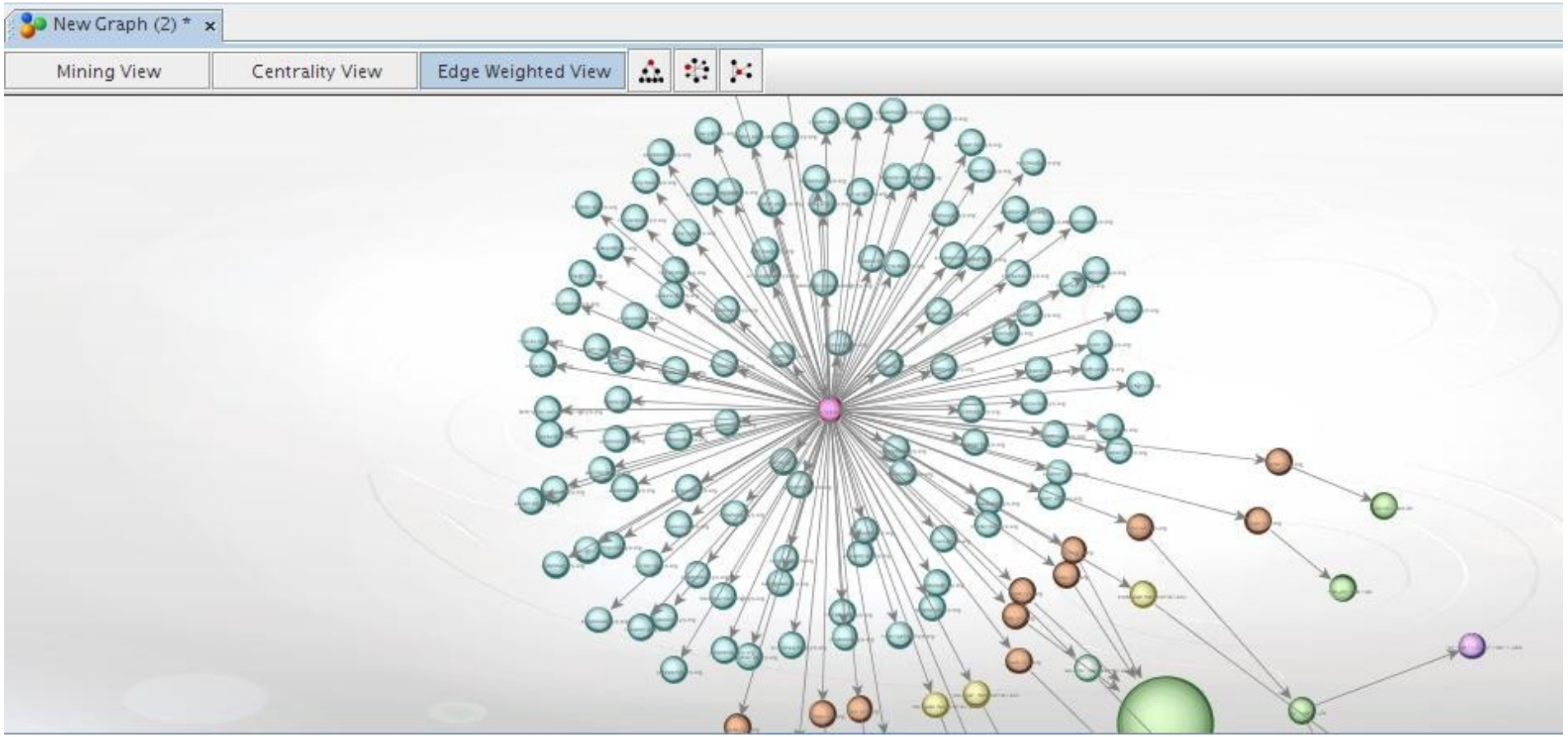
- You can also harvest phone numbers for those users.

Maltego

- See shared domains

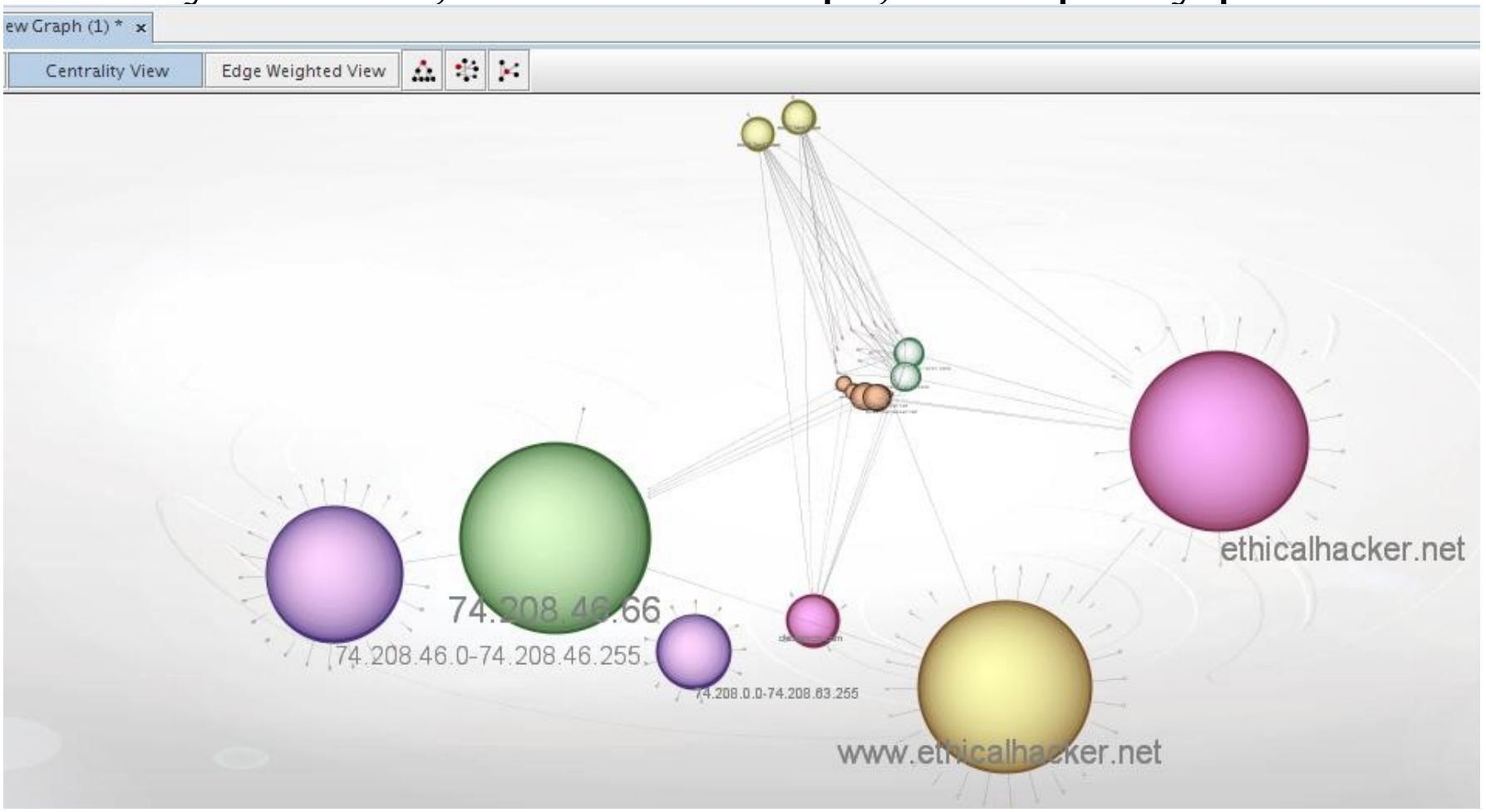
Maltego

- Sort your view, see relationships, make pretty pictures.



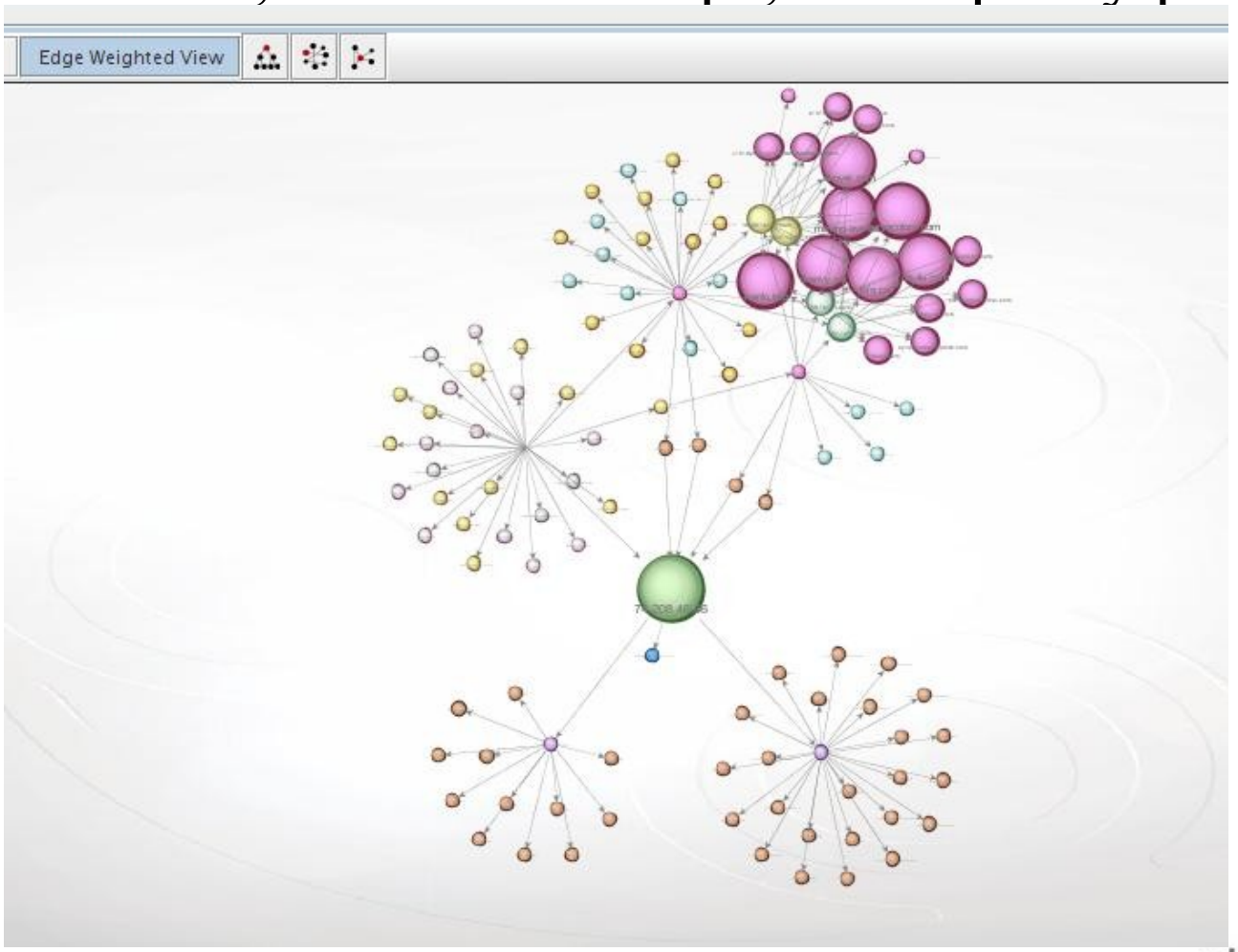
Maltego

- Sort your view, see relationships, make pretty pictures.



Maltego

- Sort your view, see relationships, make pretty pictures.



Maltego

- What else can Maltego do?
  - Technorati transforms, blog tags, search blogs for phrases
  - Incoming links, who links to your domain
  - Social network transforms
  - Can print the graphs now
  - Can export the data into .csv, can save the maltego file and be opened by any other maltego instance
  - Can write your own transforms or stand up your own server.

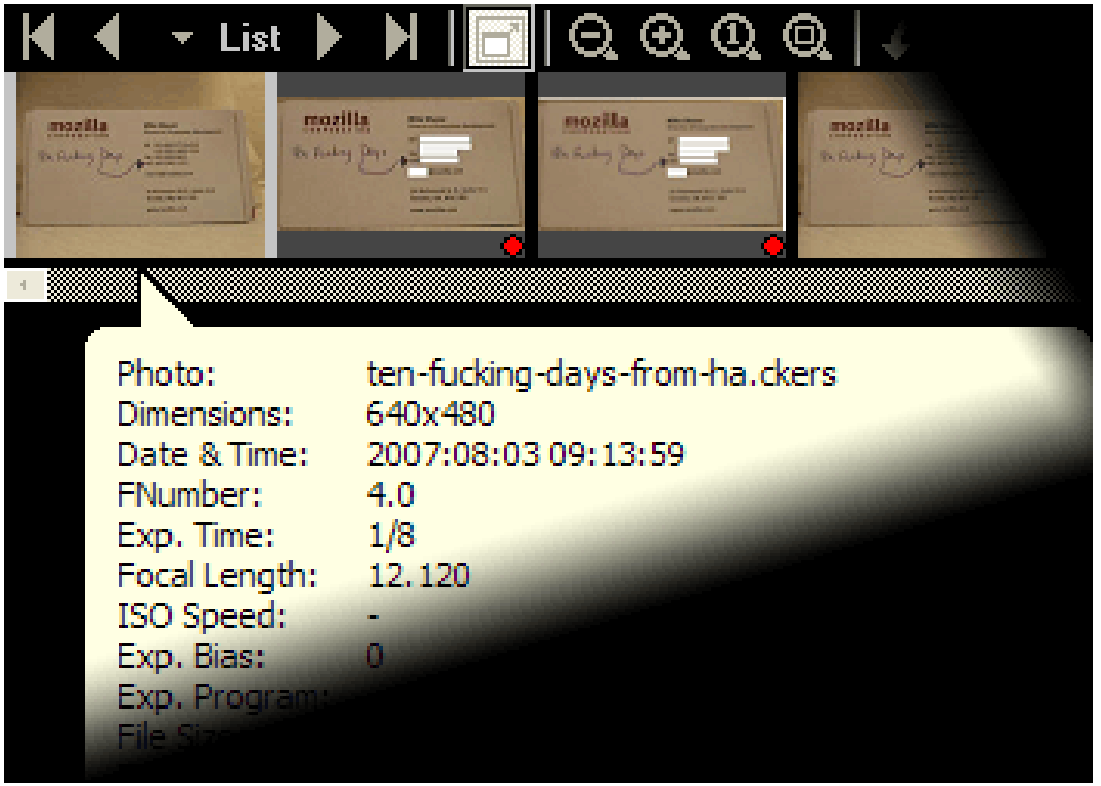
  - ** version 2 is for pay but cheap $430 USD for first year

Other Stuff--Exif metadata

- Information from jpeg metadata
  - Can tell us time, location, camera type from images, put a person at a specific place at time (sort of –only as accurate as the camera time)
  - Useful? Maybe
  - Sometimes unaltered original photo can be found in thumbnail
  - Online exif viewer
    - http://regex.info/exif.cgi

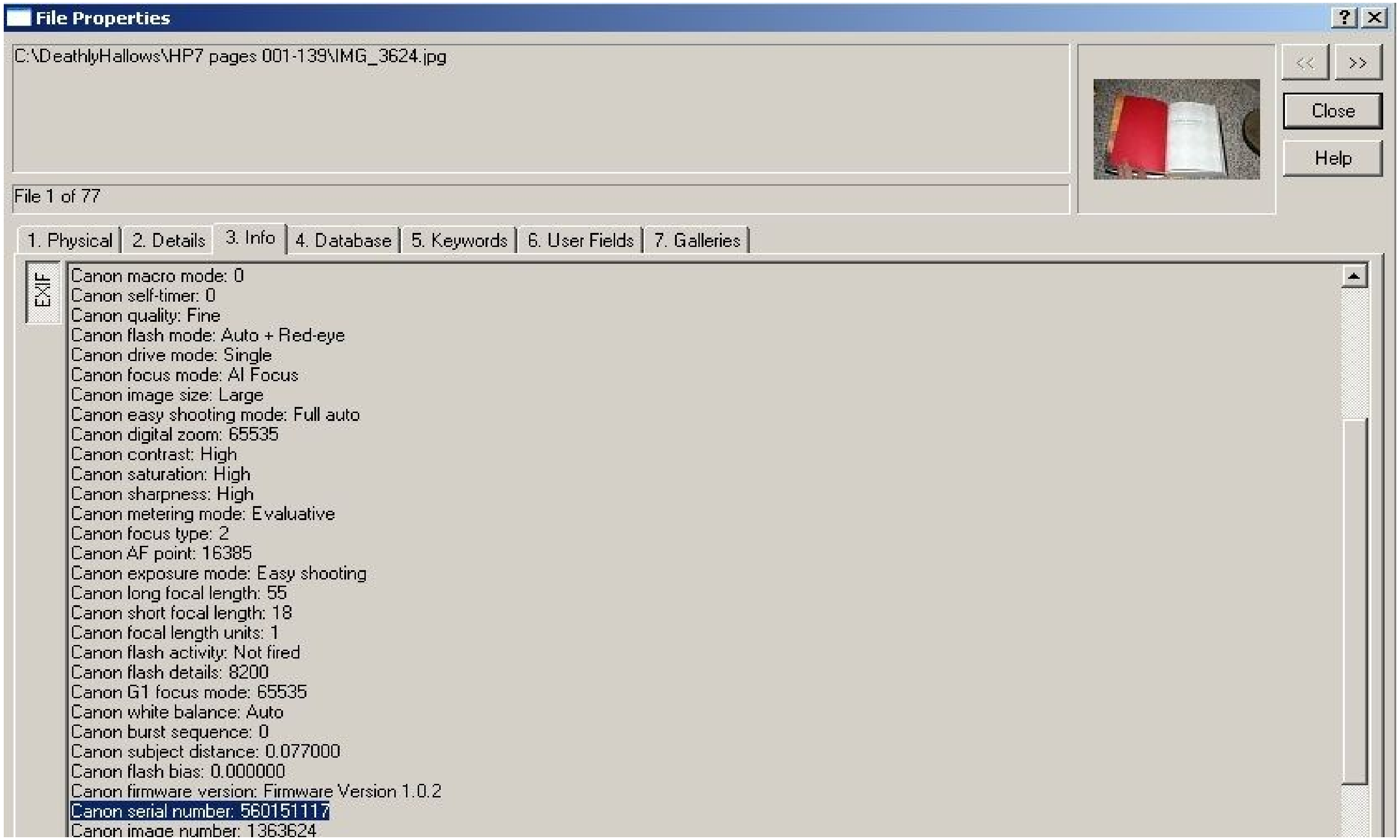
Exif metadata

- Information from jpeg metadata
- http://hackademix.net/2007/08/05/two-faces-sa



Exif metadata

- Information from jpeg metadata
- Harry Potter book leakage and camera serial #



CarnalOwnage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR
CA# 94-1720 CRR

So What?

- Ok lots of information what did I get from all of it?
  - If you are allowed to send social engineered emails or do client side attacks, you have an initial target list of email addresses. Using email dossier/maltego I can verify working email addresses. I only need one person to open/click that email for my foothold.
  - Naming conventions, users and offices, phone numbers, relationships between organizations
  - Target organization's IP Space and footprint. VPN server's IP, Terminal/Citrix server IPs, firewall's IP, etc.
  - Software versions of software that is typically targeted in client side attacks (MS office)
  - Using Maltego we see the relationships between our site and other sites in addition to the above.
  - All gained without your typical definition of "scanning"

Questions?

Chris Gates (CG)
http://carnal0wnage.blogspot.com
http://www.learnsecurityonline.com

Carnal0wnage