

**CONFIDENTIAL**

REC-21  
EX-110  
105-45325-  
Dear [REDACTED]  
Your letter  
your interest in writing  
It was  
observations on the  
want to thank you for

WARNING: SPECIAL ACCESS REQUIRED

# CONFIDENTIAL INFORMATION

File Name:

**CARNAL OWNAGE**

File No:

Earn Money  
Doing What  
You Love!

WARNING: SPECIAL ACCESS REQUIRED

**TOP SECRET**

THROTTLE LEVER  
A-65 engines have a 1210 "over 12" radius. A one to one  
ratio for the control provides a good feel and sensitivity.



HOW IT WORKS -  
EMBED AS SHOWN  
KNURLED WHEEL  
IS JUST CAUSING  
METALL SAFETY  
KNUT ON BACK.  
NEW UNTIL LATER  
ALL, HENCE MEN  
ADJUST THE  
ADJUSTER ALLING OFF.

WAG-ARE HAS A CABLE  
WHICH SHOULD BE  
a copy  
separate to  
problem in  
real telephony  
and we will have  
the encryption  
options can be  
the meantime. (TS)

Scovcroft  
Scovcroft

Declassified on 10/20/96  
under provisions of E.O. 12958  
by J. Sanders, National Security Council

# New School Information Gathering

CG

[chris@learnsecurityonline.com](mailto:chris@learnsecurityonline.com)



# Who Am I?

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

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# 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

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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)

CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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

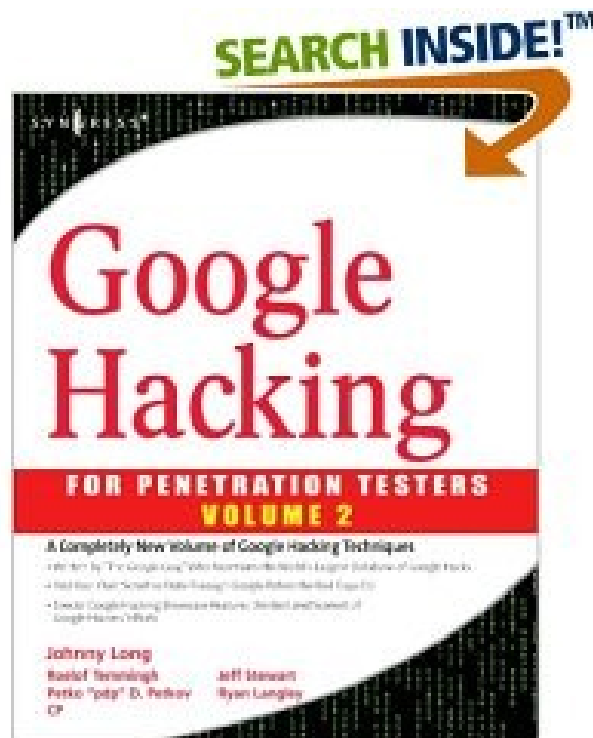
CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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.



Carnal Ownage

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# 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

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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!

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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

CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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

Carnal O w n a g e

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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.”

C a r n a l O w n a g e

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# 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.

C a r n a l O w n a g e

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Fierce DNS

- Examples...

Carnal Ownage

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Search Engine Tools

Carnal Ownage

11/10/94  
Declassified by 5668 b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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 steroids ☺

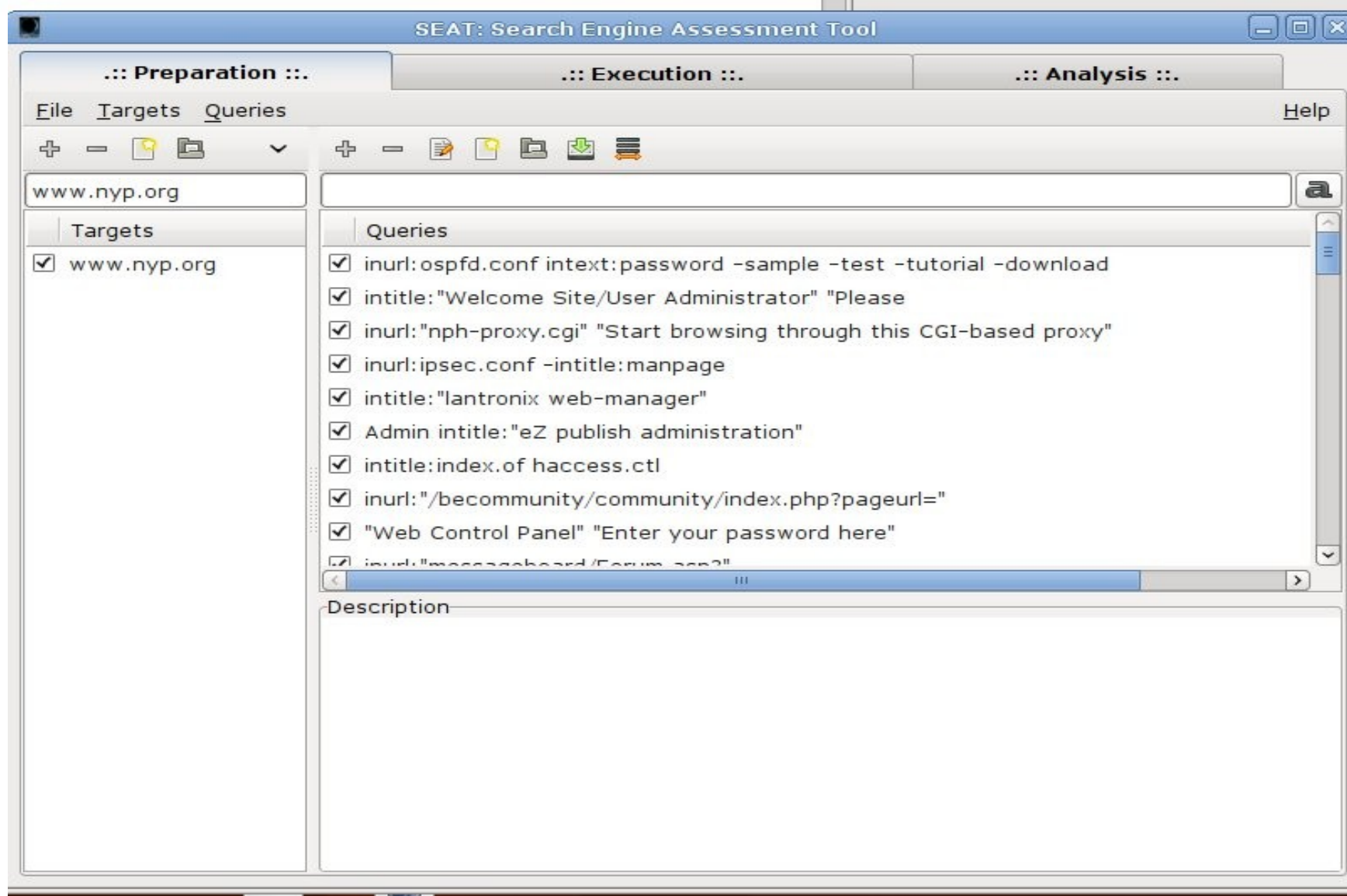
CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# SEAT (Search Engine Assessment Tool)



Carnal Ownage

11/10/94  
Classified by 5668  
Declassify on: OADR  
CA# 94-1720 CRR b7c



# SEAT (Search Engine Assessment Tool)

SEAT: Search Engine Assessment Tool

Preparation

Execution

Analysis

FileTargetsQueriesSearch EnginesMinedHelp

Targets

Queries

Search Engines

Mined

Results

Statistics

www.learnsecurityonline.com

☐ inurl:ConnectComputer/precheck.htm | inurl:Remote/logon.asp

☐ intext:"d.aspx?id" || inurl:"d.aspx?id"

☒ "Incorrect syntax near"

☐ "Certificate Practice Statement" filetype:PDF | DOC

☐ intitle:"Live View / - AXIS" | inurl:view/view.shtm

☐ "please log in"

☐ ("Fiery WebTools" inurl:index2.html) | "WebTools enable \* \*

☐ inurl:"dispatch.php?atknode&type" | inurl:class.at

MSN

www.learnsecurityonline.com

http://www.learnsecurityonline.com/index.php?option=com\_mamb

Hits: 7

Mined: 1

Results: 1

CarnalOwne

Classified by 5668  
Declassify on: OADR  
CA# 94-1720 CRR b7c



# Goolag

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

C a r n a l O w n a g e

11/10/94  
Declassified by 5668 b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Goolag

GoolagScanner Beta - (1418 dorks loaded)

File Edit Scan Tools Help

Available Dorks

Dorks

Advisories and Vulnerabilities (216)

Error Messages (68)

Files containing juicy info (228)

Files containing passwords (137)

Files containing usernames (15)

Footholds (21)

Pages containing login portals (232)

Pages containing network or vulnerability data (59)

Sensitive Directories (60)

Sensitive Online Shopping Info (9)

Various Online Devices (202)

Vulnerable Files (54)

Vulnerable Servers (46)

Web Server Detection (71)

Host: nyp.org

Scan Stop

Dork Info

"Powered by UPB" (b 1.0)(1.0 final)(Public Beta 1.0b)

"Powered by UPB" (b 1.0)(1.0 final)(Public Beta 1.0b)

dork: "Powered by UPB" (b 1.0)(1.0 final)(Public Beta 1.0b)

this is a very old vulnerability discovered by Xanthic, can't find it in GHDB and I am surprised of how it still works...

Results

Status	Dork	URL found
Scan...	"Powered by PHP Advanced ...	...
Scan...	"powered by php icalendar" -i...	...
Scan...	"powered by php photo album...	...
Scan...	"powered by PhpBB 2.0.15" -...	...
Scan...	"Powered By phpCOIN 1.2.2"	...
Scan...	"Powered by PHP-Fusion v6....	...
Scan...	"powered by phplist"   inurl:"lis...	...
Blocked	"Powered by PowerPortal v1.3"	http://sorry.google.com/sorry/?continue=http://www.google.com/search?q=%2
Scan...	"powered by pppblog v 0.3.(.)"	...
Scan...	"powered by runcms" -runcms...	...
Scan...	"powered by sblog" +"version...	...
Scan...	"Powered by sendcard - an a...	...
Scan...	"Powered by Simplog"	...
Scan...	"powered by sphider" -exploit ...	...
Scan...	"powered by ubbthreads"	...
Scan...	"Powered by UPB" (b 1.0)(1....	...

CarnalOwne

Classified by 3645  
Declassify on: OADR  
CA# 94-1720 CRR

b7c



# Email Harvesting

Carnal Ownage

11/10/94  
Declassified by 5668 b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# 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)

CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Google Mail Harvesters

- Goog-mail.py

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Google Mail Harvesters

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

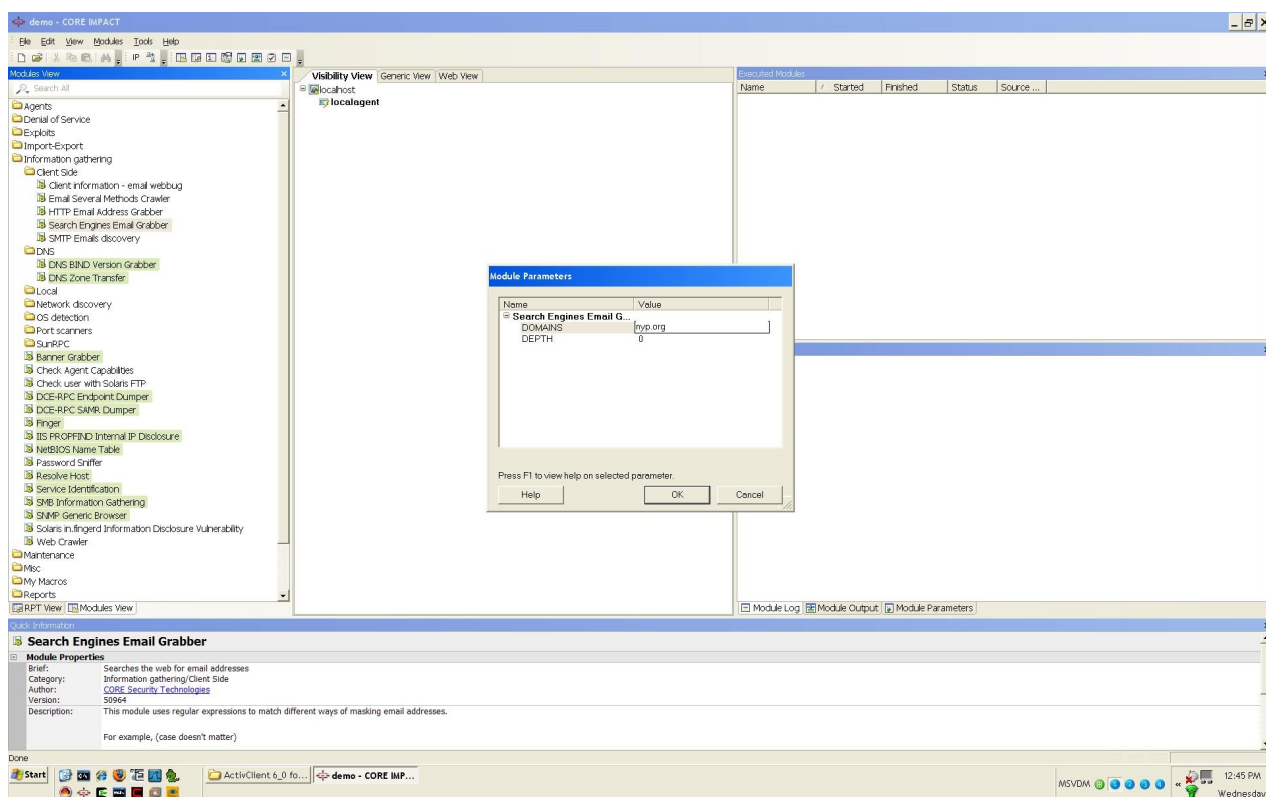
C a r n a l O w n a g e

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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.



Carnal Ownage

11/10/94  
Classified by 57648 [redacted] b7c  
Declassify on: OADR  
CAF 94-1720 CRR



# 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 ☺

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# Document Metadata Extraction

Carnal Ownage

11/10/94  
Declassified by SP6/8 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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.

CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Metagoofil

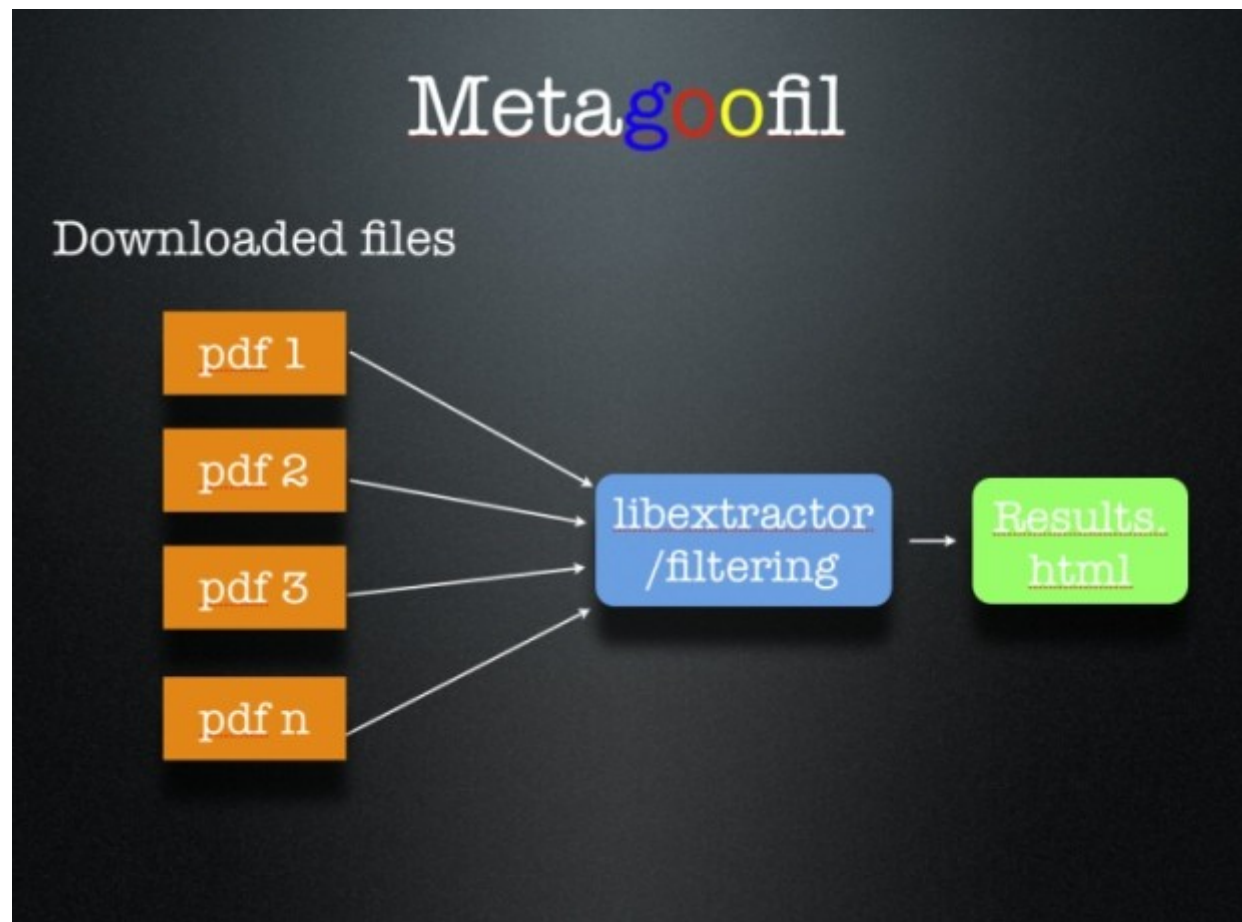
- “It will generate a html page with the results of the metadata extracted, plus a list of potential usernames and path disclosure, can be useful for preparing a bruteforce attack on open services like ftp, pop3, web applications, vpn, etc.”

CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Metagoofil



Carnal Overage

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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](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 Overage

11/10/94  
Classified by 5668 [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.

CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# On-line Tools

Carnal Ownage

11/10/94  
Declassified by SP6/ef [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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.

CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Netcraft

Whats that site running?

## 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



(c) Netcraft, [www.netcraft.com](http://www.netcraft.com)

CarnalOwne

11/10/94  
Classified by 5668  
Declassify on: OADR  
CA# 94-1720 CRR b7c



# ServerSniff.net

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

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# ServerSniff.net

- AS Reports

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# ServerSniff.net

- Subdomains

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# ServerSniff.net

- Hostnames on an IP

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# ServerSniff.net

- Hostnames on a DNS server

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# ServerSniff.net

- Web Tools

Domain - reports and all about ips, networks and dns - Windows Internet Explorer

http://serversniff.net/httpheader.php

Learn Security Online - Home Domain - reports and all ... x http://metasploit.com/data/...

Home	Reports	IP-Tools	Nameserver	Webserver	Crypto	Other Tools	Impressu
------	---------	----------	------------	-----------	--------	-------------	----------

DEUTSCH

- SSL - Info
- Header
- Page-Source
- Hyperlinks on Page
- Comments on Page
- robots.txt
- File-Search
- File-Info

Method Hostheader URI TO Headers

seffnet

CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# ServerSniff.net

- Web Tools (Show hyperlinks in a page)

CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# ServerSniff.net

- Web Tools (Show comments in HTML)

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# ServerSniff.net

- Web Tools (Show HTML Source)

CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# ServerSniff.net

- Web Tools (web server headers)

CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# ServerSniff.net

- Web Tools (SSL information)

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# DomainTools.com

- <http://www.domaintools.com/>



Wildcard search of all current/deleted/expired whois domains.  
Domain Suggestions Engine serves over 10 Billion suggestions a year.

DomainTools Live Auction closing NOW! [Bid Now!](#)

[Whois](#) [Suggestions](#) [Domain Search](#) [At Auction](#) [For Sale](#) [DNS Tools](#)

Whois Lookup:

 **DOMAIN ROUNDTABLE CONFERENCE**  
"Welcome to The New Domain Industry"

Do you own high-quality generic domains? [List them](#) in the April 21st DomainTools Live Auction at the Domain Roundtable Conference in San Francisco. Want to ensure your domain is listed? [Register now](#) for the conference - every attendee has a guaranteed-acceptance slot of one domain in the Live Auction.

  - [Sign up for the Roundtable.](#)

Our Latest Blog Post: [DomainTools Live Auction](#) - 9 comments

 <a href="#">More Tools and Services</a> Complete collection of all tools.	 <a href="#">Domain History</a> Whois history database.	 <a href="#">Mark Alert</a> Alerts when a domain uses my trademark.
 <a href="#">Live reports on web hosting companies</a> Detailed uptime reports on providers	 <a href="#">Name Intelligence Awards</a> The 2007 awards are out, see who won.	 <a href="#">Reverse IP</a> Patent pending reverse IP search.
 <a href="#">DNS Tools</a> DNS stuff, whois, traceroute, and ping.	 <a href="#">Members Area</a> Modify account settings and options.	 <a href="#">Name Server Spy</a> Follow the transfers of a name server.
 <a href="#">Domain Monitor</a> Free tool to monitor all my domains.	 <a href="#">Typo Generator</a> Find Domain Typos on any Domain.	 <a href="#">Whois Applications and Toolbars</a> Google toolbar add-on and other applications.

CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# DomainTools.com

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

DomainTools Live Auction starts closing in about...  
4 days 1 hour 3 mins 29 secs

Whois ▶ Domain Suggestions ▶ For Sale ▶ Auctions ▶ Advanced Auctions ▶

Domain Directory Ping ▶ Traceroute ▶ My IP Address Domain Parking **Beta** Cheap Domain Name Regis

**Power Tools:** Reverse IP Domain History Mark Alert Name Server Spy Hosting History Regi

Reverse IP - View all domain names hosted on an IP address

## Look an IP Address

Enter an IP address or domain name into the form below and click "Look Up" to get a list of domains hosted on the same IP address.

IP/Domain Name:

ethicalhacker.net

Look Up

Example: 192.168.% or 64.233.161.104

There are 8 domains hosted on this IP address.

Here are a few of them:

1. [Cawffee.com](#)
2. [Certifiedsecuritypro.com](#)
3. [Chicagocon.com](#)
4. [5 more...](#)

CarnalOwne

Classified by 5668  
Declassify on: OADR  
CA# 94-1720 CRR b7c



# DomainTools.com

- Hosting history for EH.net

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:

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	<a href="#">63.251.163.115</a>	-none-
2004-09-29	New	-none-	<a href="#">217.160.226.73</a>
2005-06-11	Change	<a href="#">217.160.226.73</a>	<a href="#">82.165.199.10</a>
2005-06-18	Change	<a href="#">82.165.199.10</a>	<a href="#">82.165.129.30</a>
2006-01-15	Change	<a href="#">82.165.129.30</a>	<a href="#">82.165.170.112</a>
2006-04-02	Change	<a href="#">82.165.170.112</a>	<a href="#">82.165.178.72</a>
2006-04-15	Change	<a href="#">82.165.178.72</a>	<a href="#">82.165.177.220</a>
2007-05-13	Change	<a href="#">82.165.177.220</a>	<a href="#">74.208.46.66</a>

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	<a href="#">eNom.com</a>
2004-09-27	<a href="#">Schlund.de</a>

### Name Server History

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

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

CarnalOwne

11/10/94  
Classified by 5668  
Declassify on: OADR  
CA# 94-1720 CRR b7c





# CentralOps.net

- <http://centralops.net/co/>

**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

**Free online network utilities**

**Domain Dossier**  
Investigate domains and IP addresses. Get registrant information, DNS records, and more.

**Domain Check**  
See if a domain is available.

**Email Dossier**  
Validate and investigate email addresses.

**Browser Mirror**  
See what your browser reveals.

**Ping**  
See if a host is reachable.

**Traceroute**  
Trace the network path from this server to another.

**NsLookup**  
Look up various domain resource records with this version of the classic NsLookup utility.

**AutoWhois**  
Get Whois records automatically for domains worldwide.

**TcpQuery**  
Grab a web page, look up a domain, and more.

**AnalyzePath**  
Do a simple, graphical traceroute.

CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# CentralOps.net

- TCP Queries

C a r n a l O w n a g e

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# CentralOps.net

- Traceroute

Carnal Ownage

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# CentralOps.net

- Whois information

C a r n a l O w n a g e

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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

CarnalOwne

11/10/94  
Classified by 5668  
Declassify on: OADR  
CA# 94-1720 CRR b7c



# CentralOps.net

- Email Verification (failure)

C a r n a l O w n a g e

11/10/94  
Declassified by 5668 b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# CentralOps.net

- Email Verification (success)

C a r n a l O w n a g e

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Clez.net

- Query port and service information

Carnal Ownage

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# Clez.net

- Query port and service information

net.app

what's up and running?

idn  :     protocol hint



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.

CarnalOwne

1/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Clez.net

- Query port and service information

net.ann

what's up and running?

idn hyp.org : 22 go ☒ Net ☐ Head



? info

scan result

port list (3)

Port closed/filtered

net.ann

what's up and running?

idn www.learnsecurityonline.com : 22 go ☒ Net ☐ Head



? info

scan result

port list (3)

Application: OpenSSH 4.2 (protocol 2.0) Protocol: ssh

CarnalOwne

11/10/94

Classified by 5668

Declassify on: OADR

CA# 94-1720 CRR

b7c



# Robtex

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

C a r n a l O w n a g e

11/10/94  
Declassified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Tying it all together with Maltego

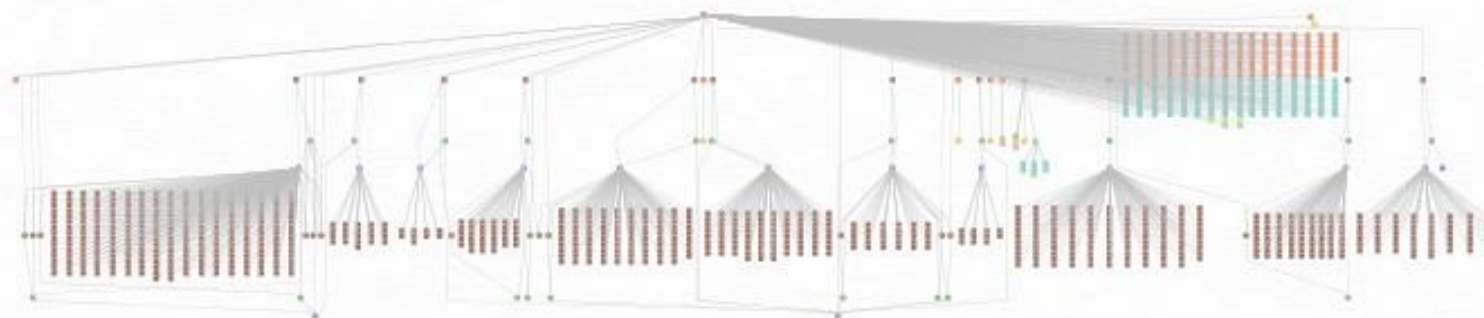
Carnal Ownage

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Maltego

- What does this tell me about our target domain?



EmailAddress   Netblock   Phrase  
PhoneNumber   NSrecord   Person  
MXrecord   Document   IPAddress  
DNSName   Domain

Carnal Ownage

11/10/94  
Classified by 57668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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)

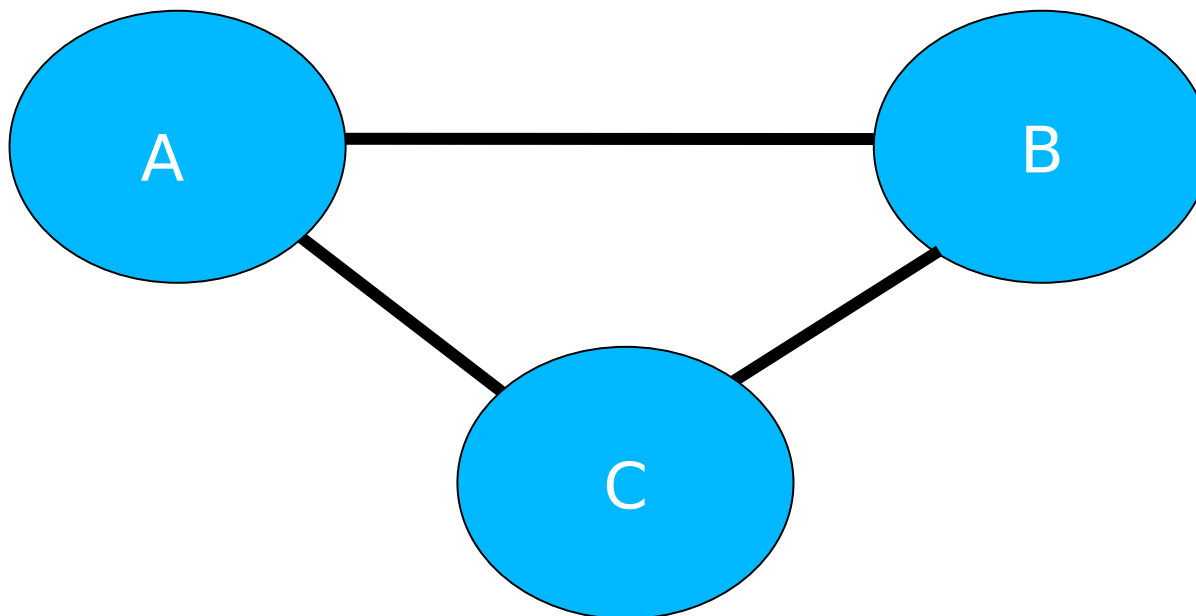
CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Maltego

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



Carnal Overage

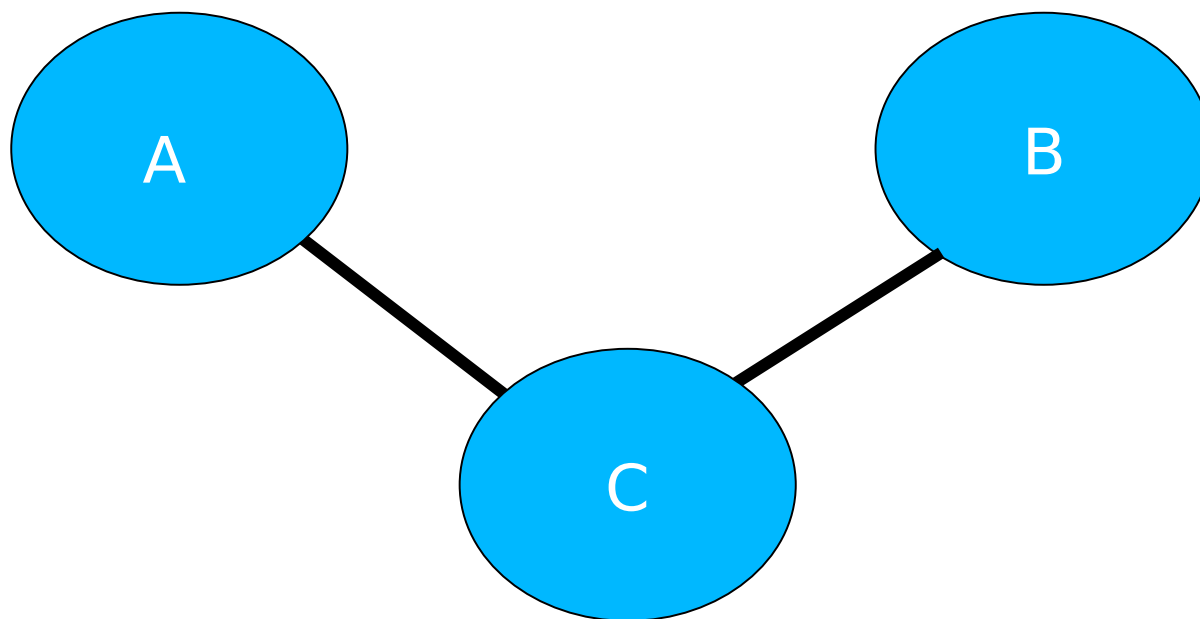
11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# Maltego

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



Carnal Overage

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Maltego

- Find our MX and NS servers

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Maltego

- See what hostnames are shared by the DNS servers

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Maltego

- Brute force our domain names and resolve them to IPs

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Maltego

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

C a r n a l O w n a g e

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Maltego

- Harvest emails for the domain and verify them.

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Maltego

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

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# Maltego

- You can also harvest phone numbers for those users.

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Maltego

- See shared domains

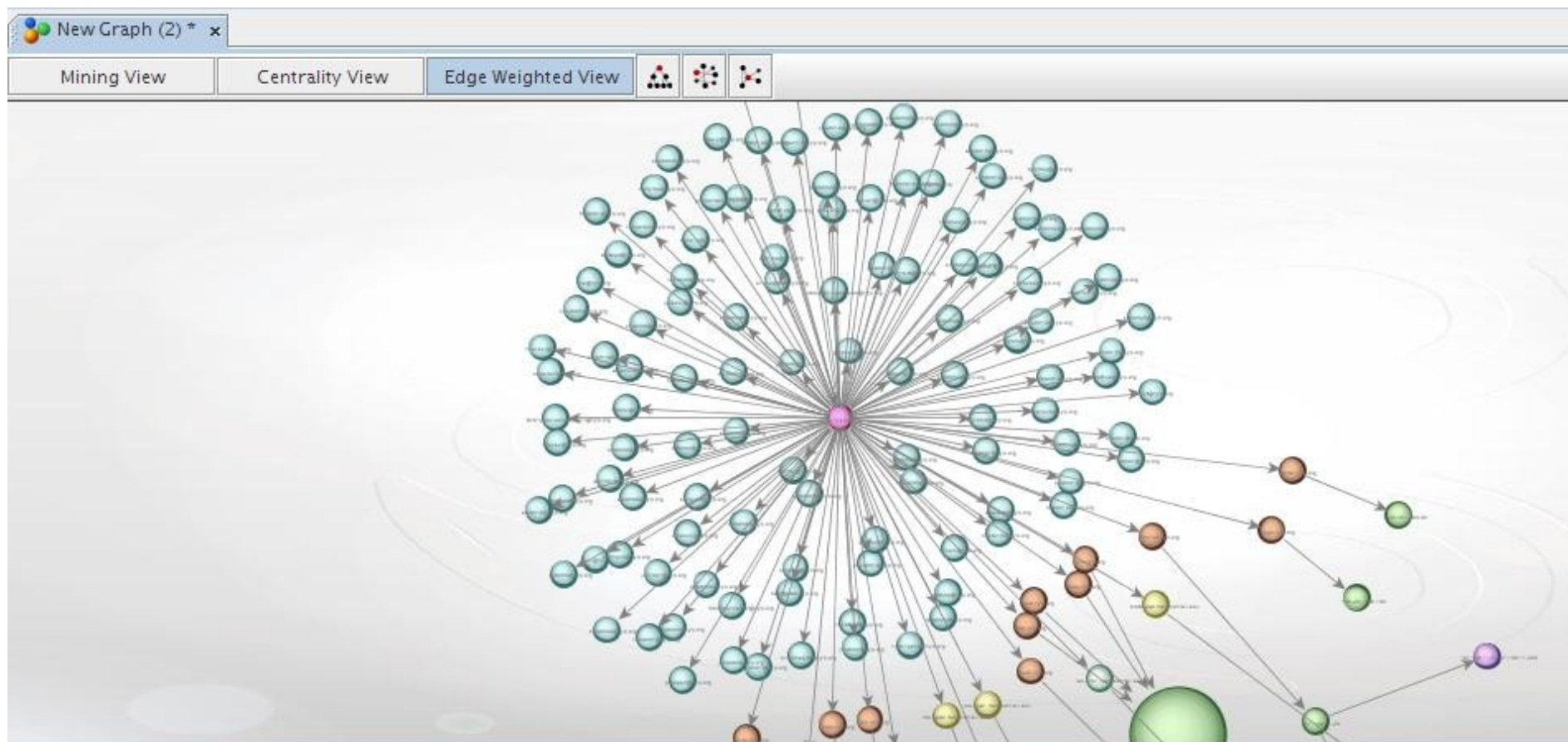
Carnal Ownage

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Maltego

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



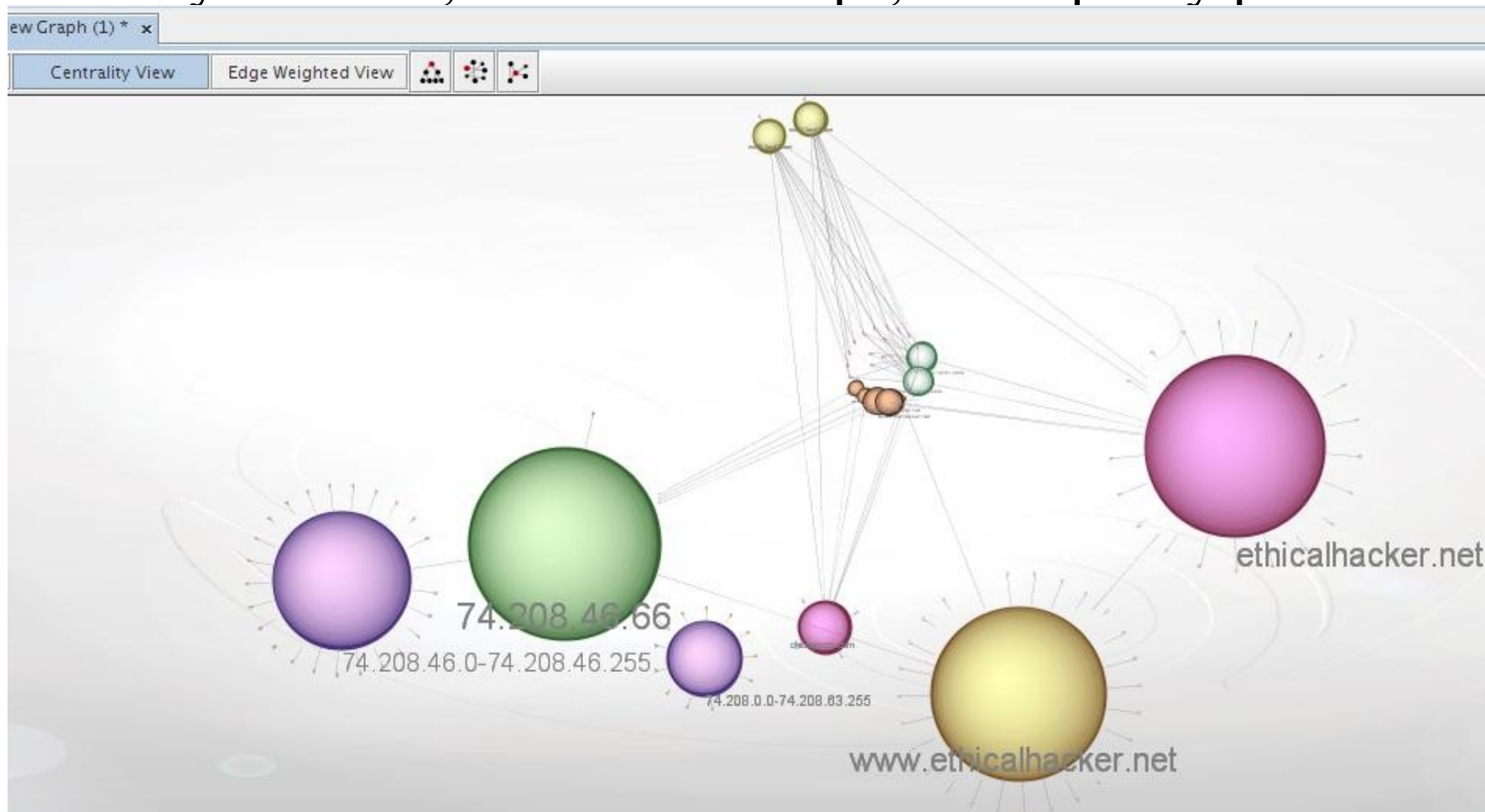
Carnal Ownage

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Maltego

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



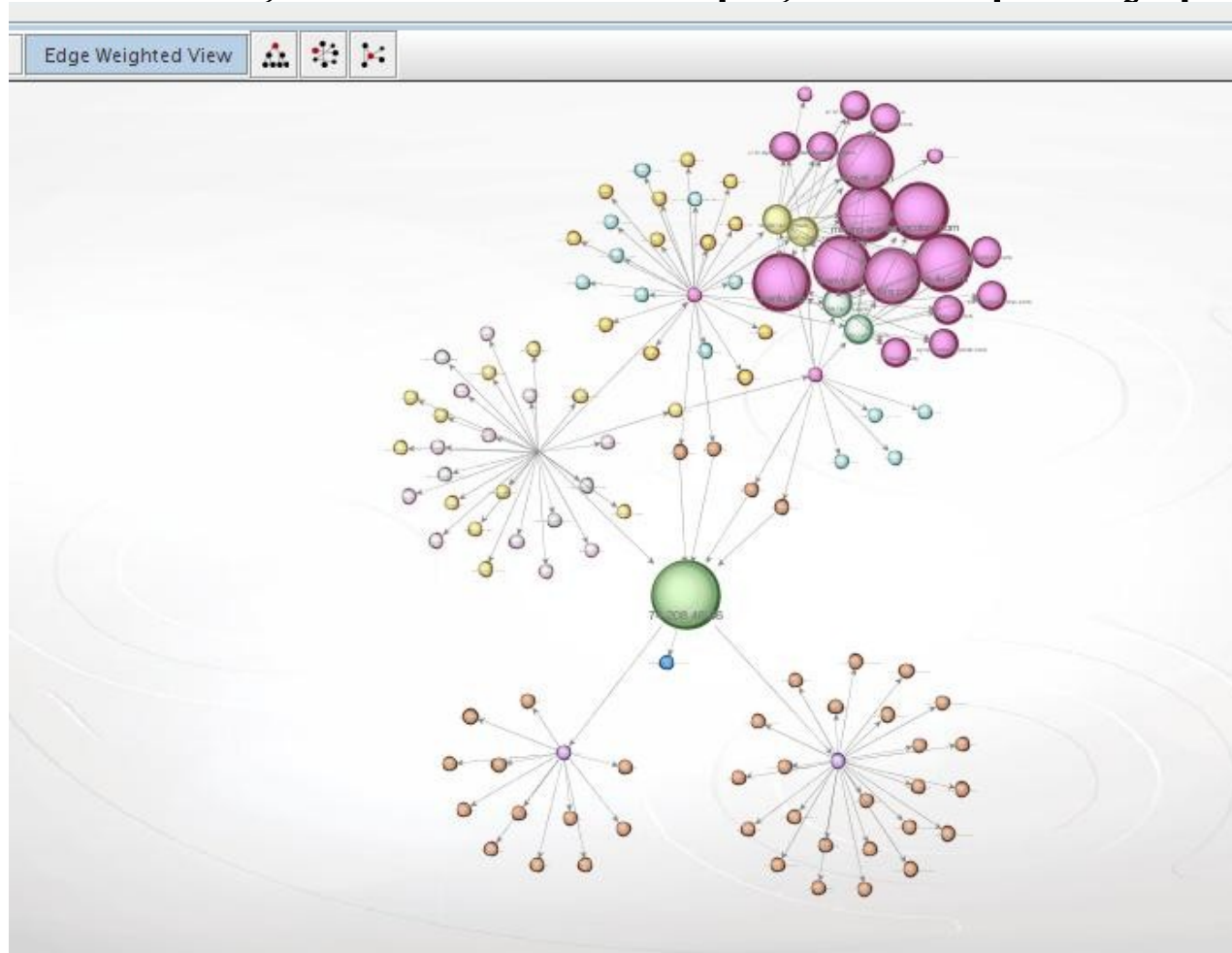
CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Maltego

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



Carnal Overage

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# 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

CarnalOwne

11/10/94  
Classified by 5668 [REDACTED] b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# 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>

Carnal O w n a g e

11/10/94  
Classified by 57648 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR





# Exif metadata

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



Photo:	ten-fucking-days-from-hackers
Dimensions:	640x480
Date & Time:	2007:08:03 09:13:59
FNumber:	4.0
Exp. Time:	1/8
Focal Length:	12.120
ISO Speed:	-
Exp. Bias:	0
Exp. Program:	
File Size:	

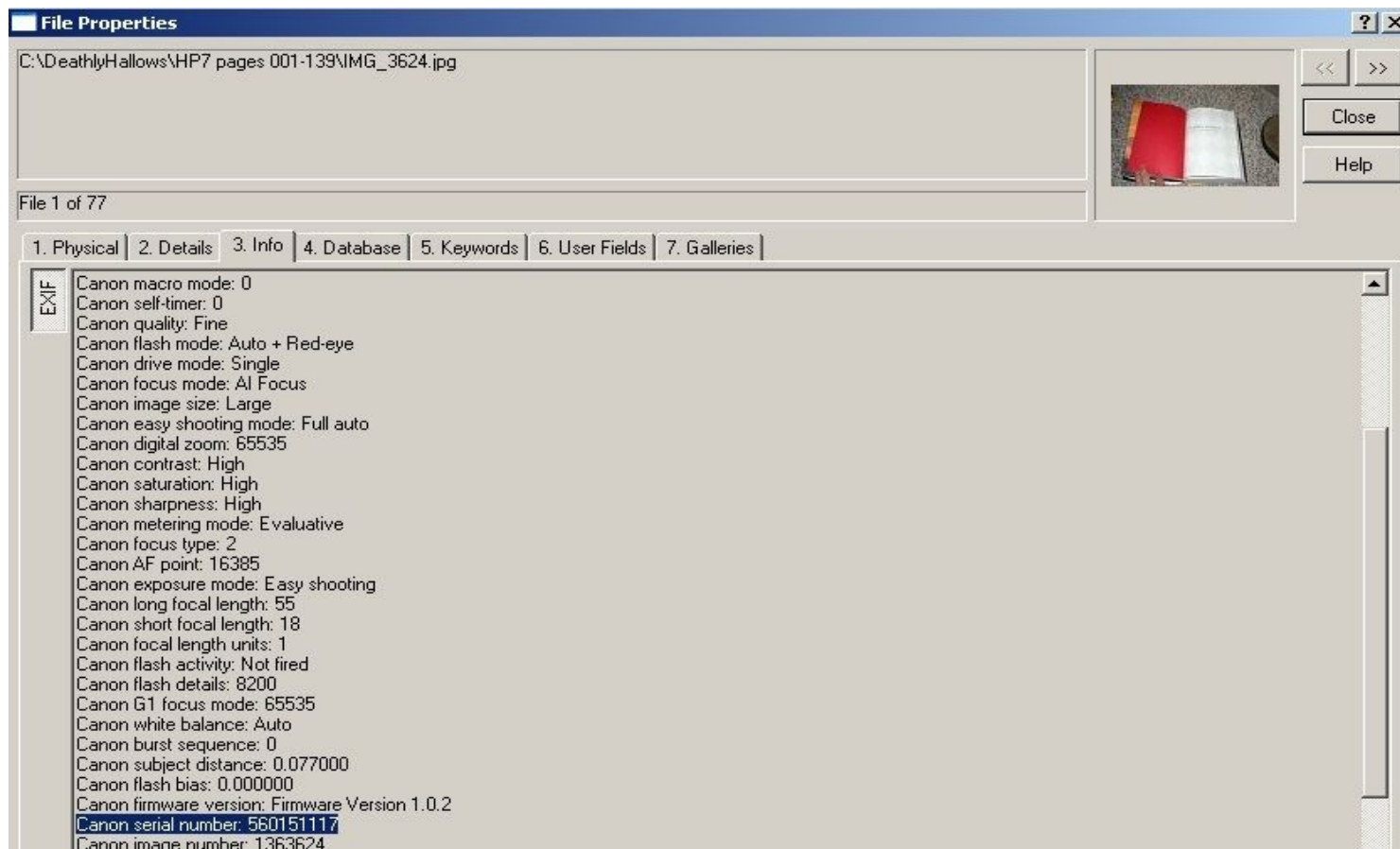
Carnal O w n a g e

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Exif metadata

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



CarnalOwne

11/10/94  
Classified by 5668 [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"

CarnalOwne

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR



# Questions?

Chris Gates (CG)

<http://carnal0wnage.blogspot.com>

<http://www.learnsecurityonline.com>

C a r n a l 0 w n a g e

11/10/94  
Classified by 5668 [redacted] b7c  
Declassify on: OADR  
CA# 94-1720 CRR