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

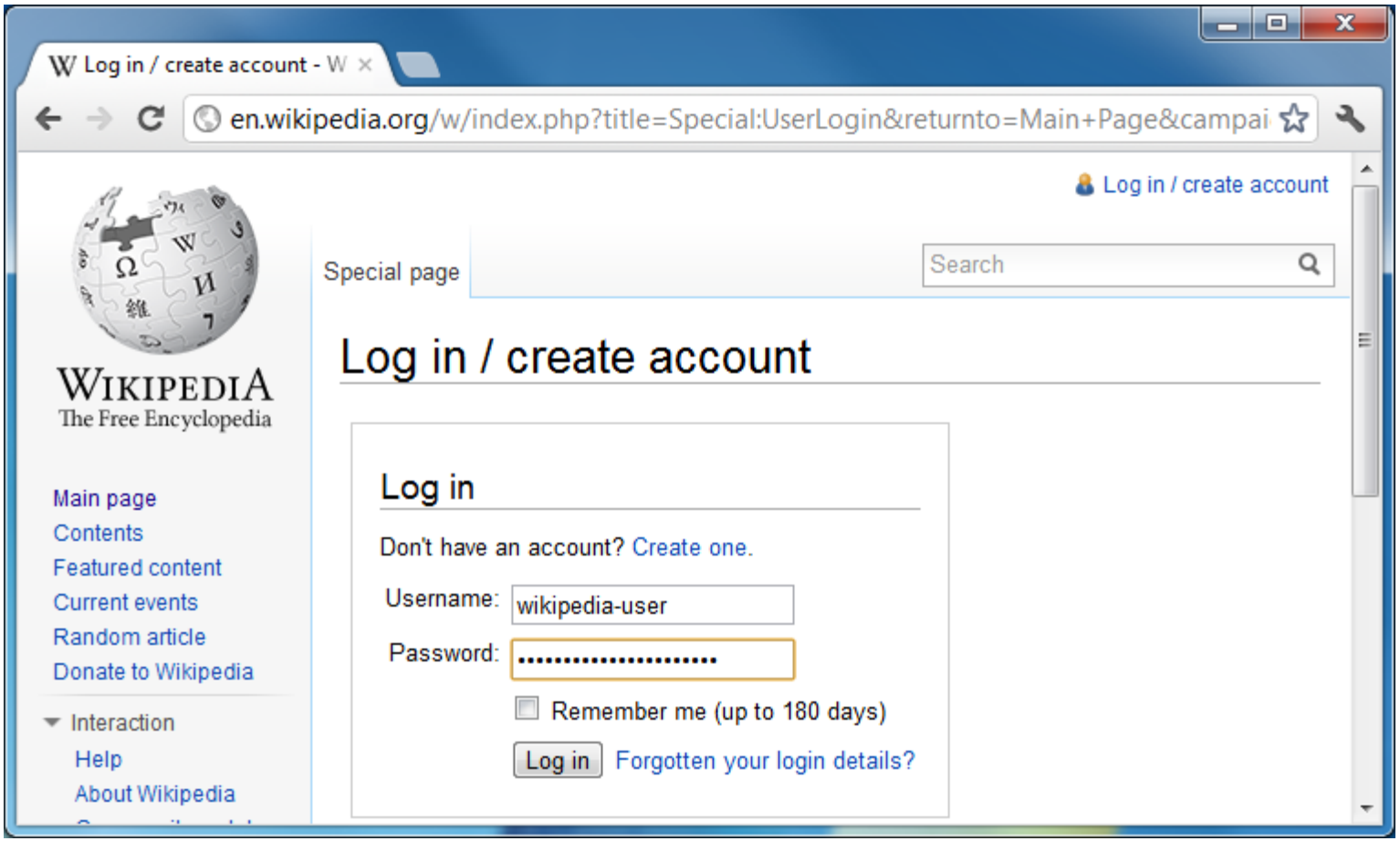
Summary

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

HTTP & HTTPS Passwords in RAM

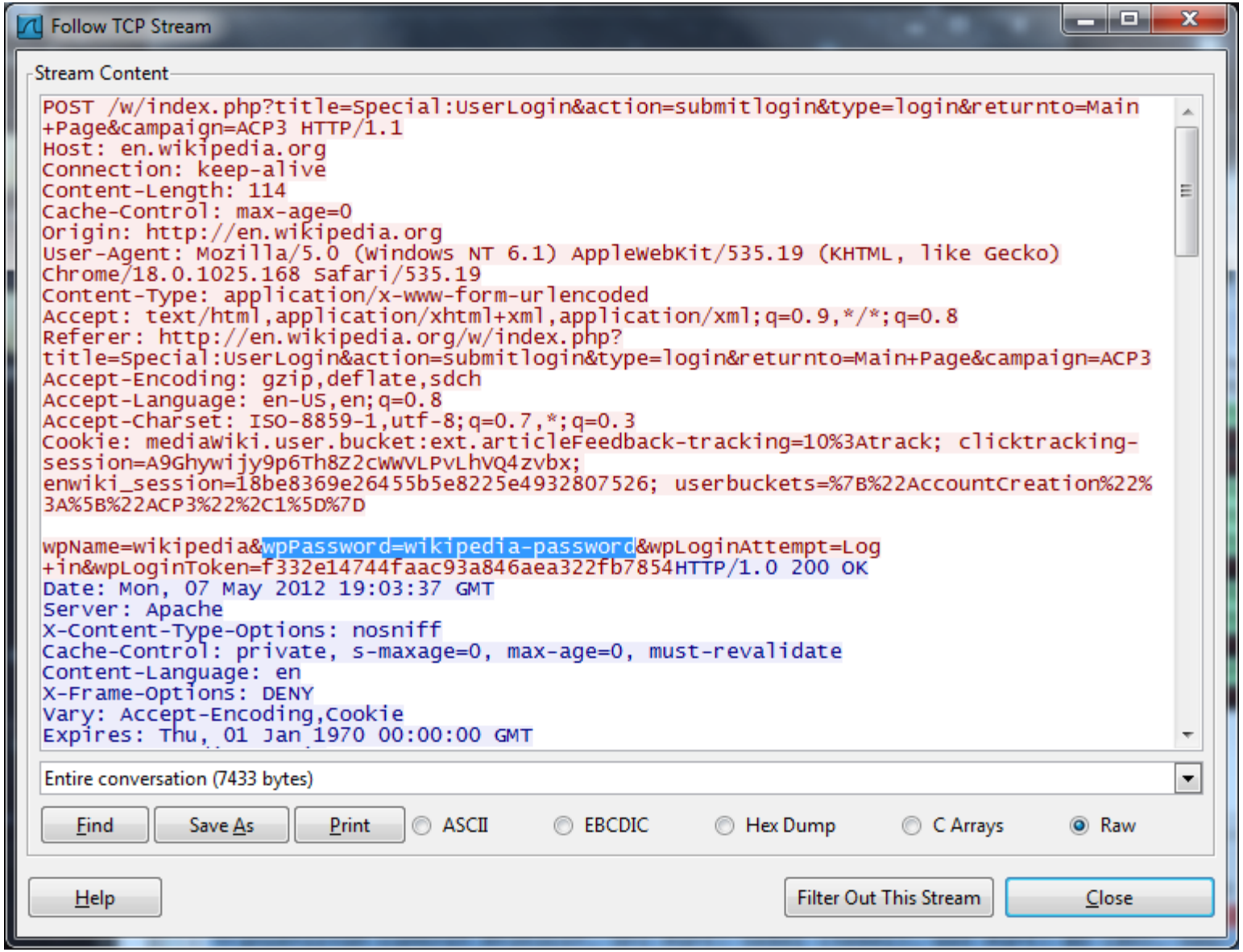
HTTP Web Login

- HTTP Authentication: Wikipedia

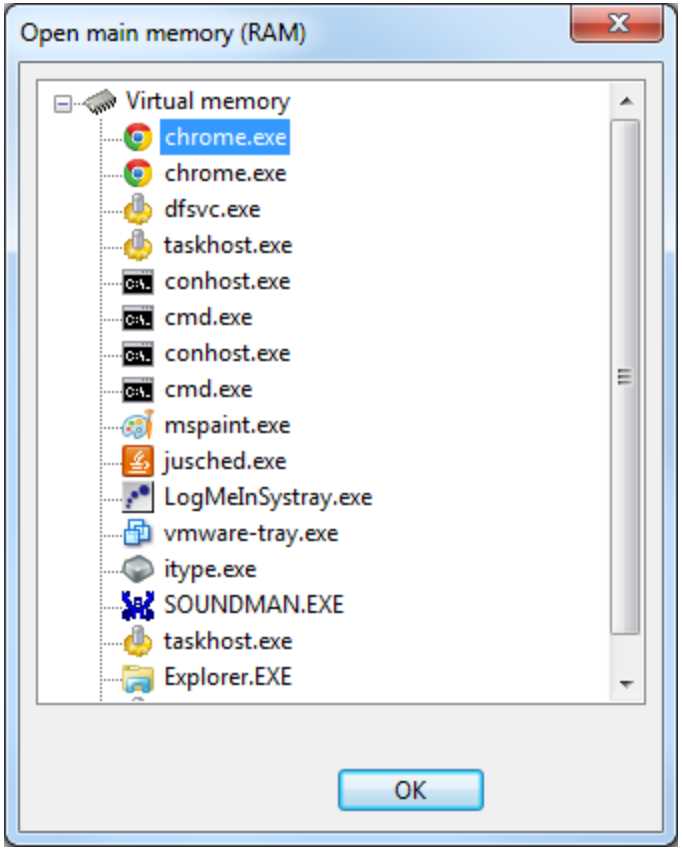


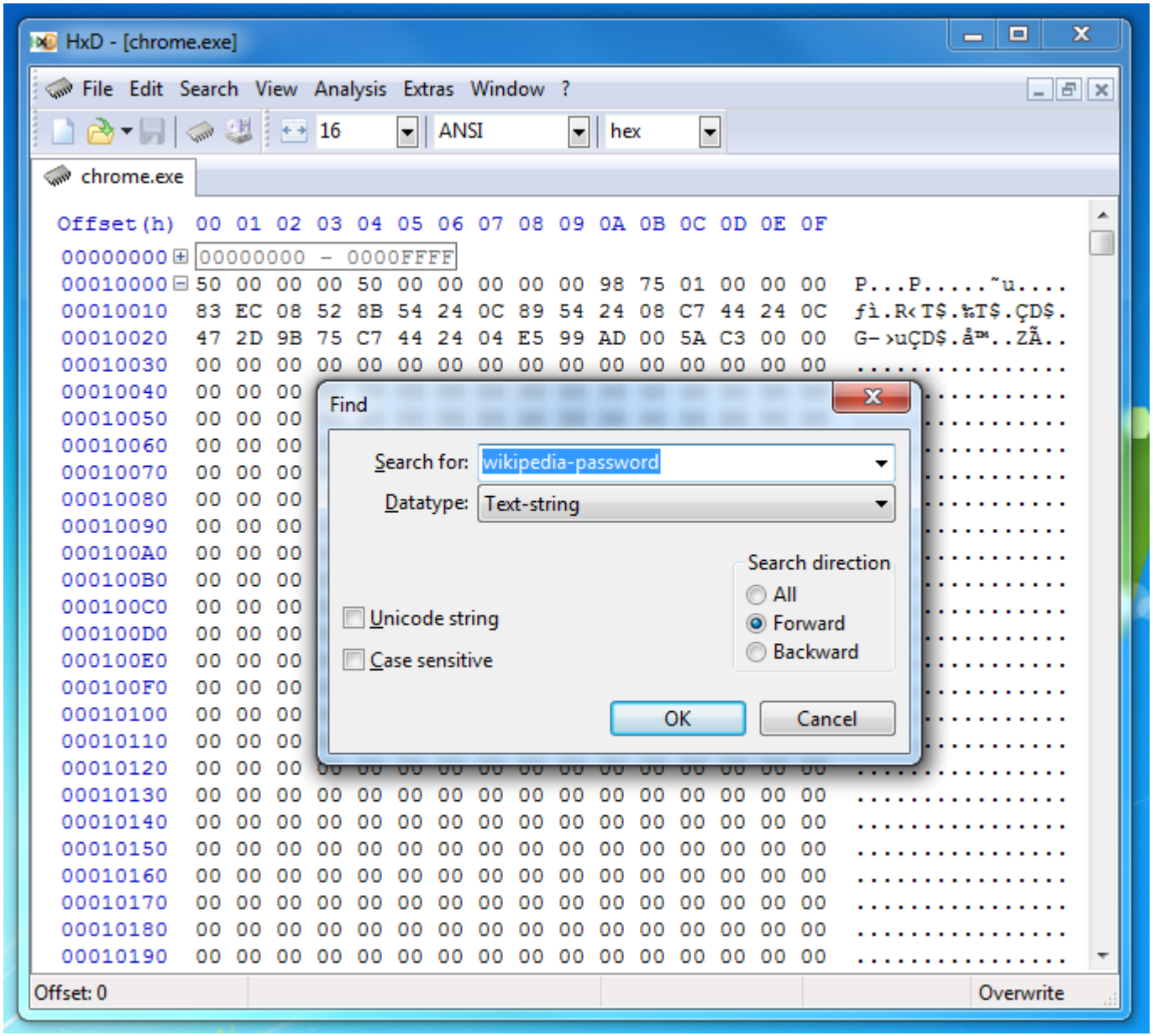
HTTP Web Login

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

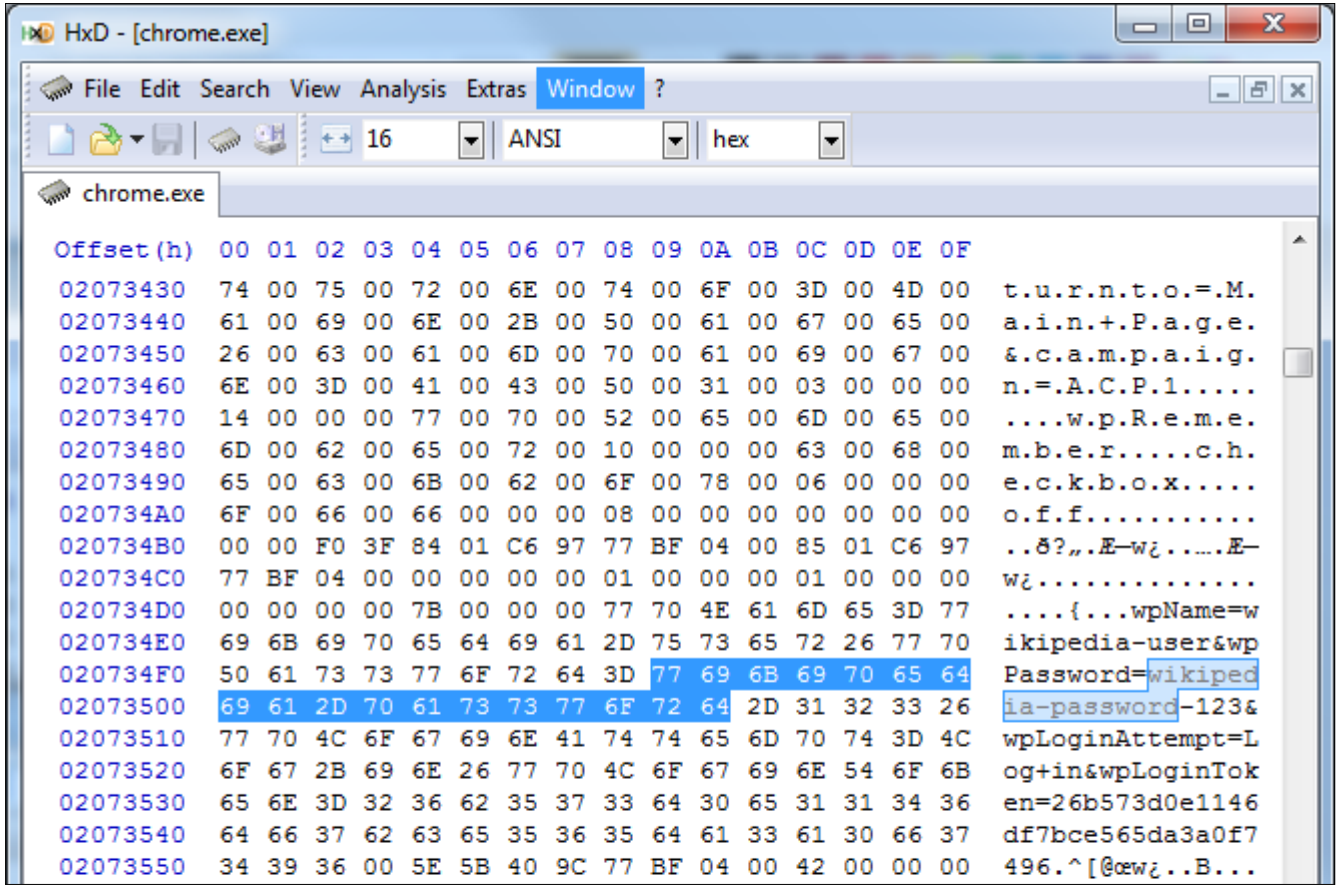

Follow TCP Stream
Stream Content
POST /w/index.php?title=Special:UserLogin&action=submitlogin&type=login&returnto=Main
+Page&campaign=ACP3 HTTP/1.1
Host: en.wikipedia.org
Connection: keep-alive
Content-Length: 114
Cache-Control: max-age=0
Origin: http://en.wikipedia.org
User-Agent: Mozilla/5.0 (Windows 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=A9Ghywijy9p6Th8Z2cWWVLPvLhVQ4zvbx;
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

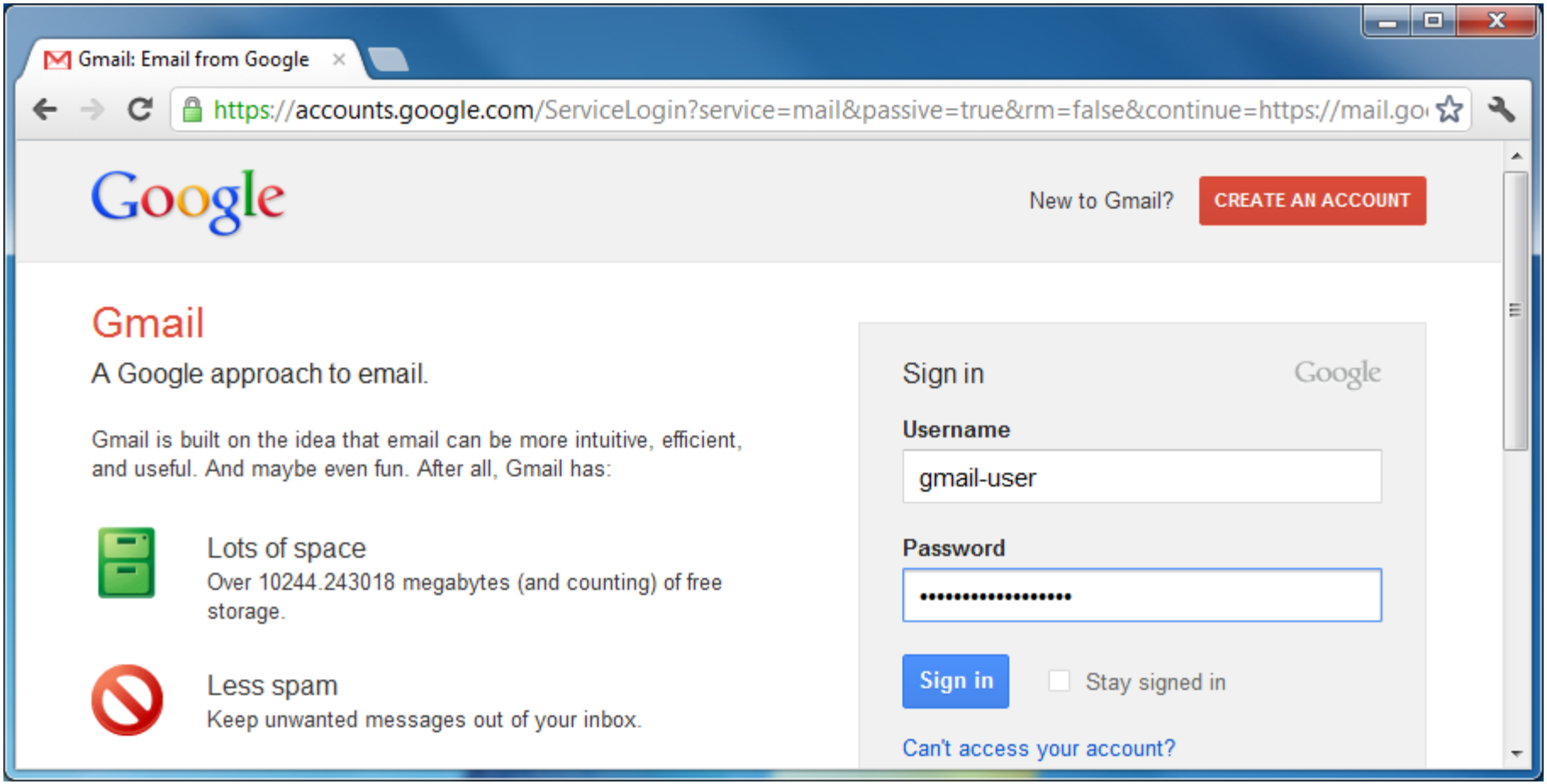



HxD - [chrome.exe]
File Edit Search View Analysis Extras Window ?
16
ANSI
hex
chrome.exe
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 00000000 - 0000FFFF
00010000 50 00 00 00 50 00 00 00 00 00 98 75 01 00 00 00 P...P.....˜u....
00010010 83 EC 08 52 8B 54 24 0C 89 54 24 08 C7 44 24 0C ƒì.R‹T$.‰T$.ÇD$.
00010020 47 2D 9B 75 C7 44 24 04 E5 99 AD 00 5A C3 00 00 G-›uÇD$.å™..ZÃ..
00010030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00010040 00 00 00
00010050 00 00 00
00010060 00 00 00
00010070 00 00 00
00010080 00 00 00
00010090 00 00 00
000100A0 00 00 00
000100B0 00 00 00
000100C0 00 00 00
000100D0 00 00 00
000100E0 00 00 00
000100F0 00 00 00
00010100 00 00 00
00010110 00 00 00
00010120 00 00 00
00010130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00010140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00010150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00010160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00010170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00010180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00010190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Find
Search for: wikipedia-password
Datatype: Text-string
Search direction
All
Forward
Backward
Unicode string
Case sensitive
OK
Cancel
Offset: 0
Overwrite

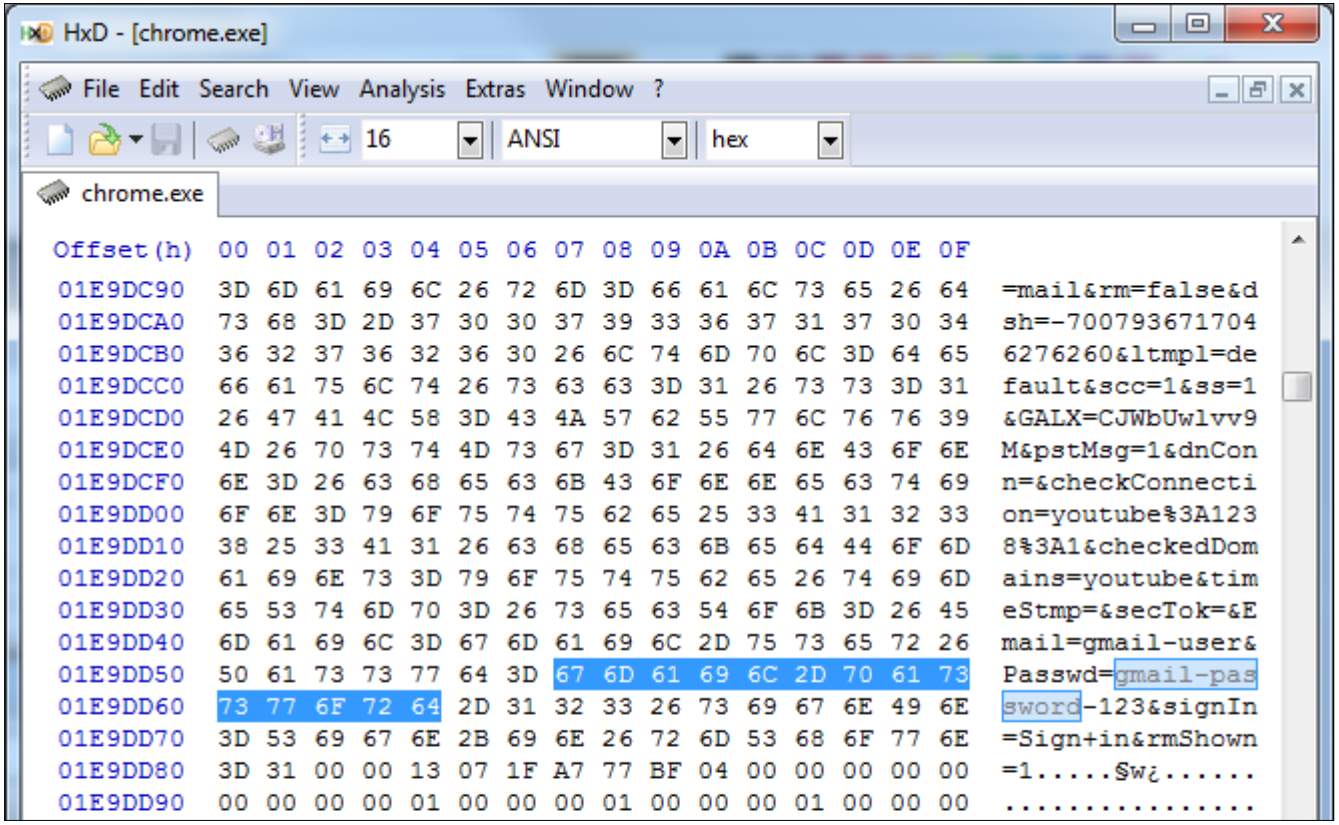
Password Found



HTTPS Web Login

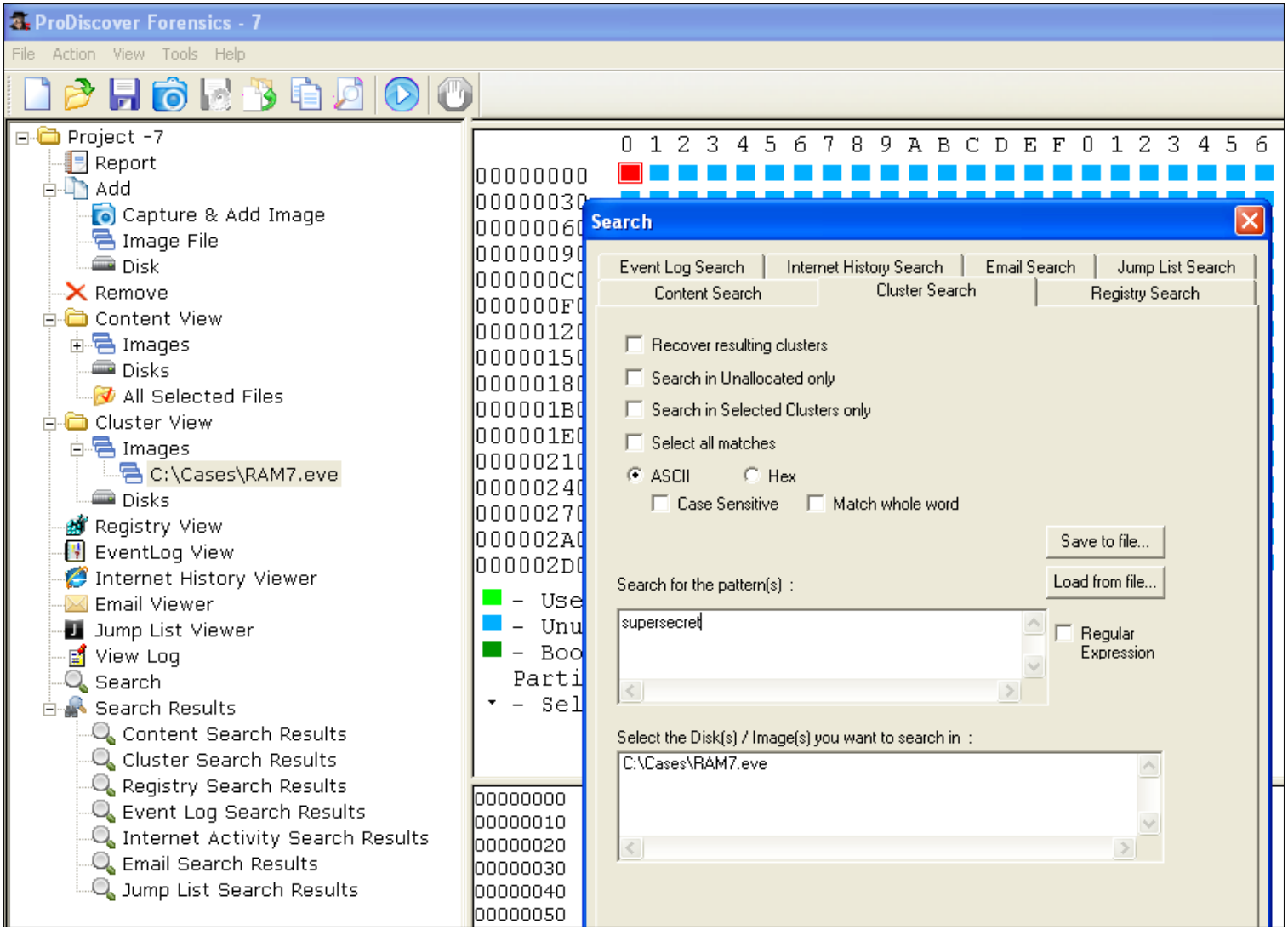


Password Found!



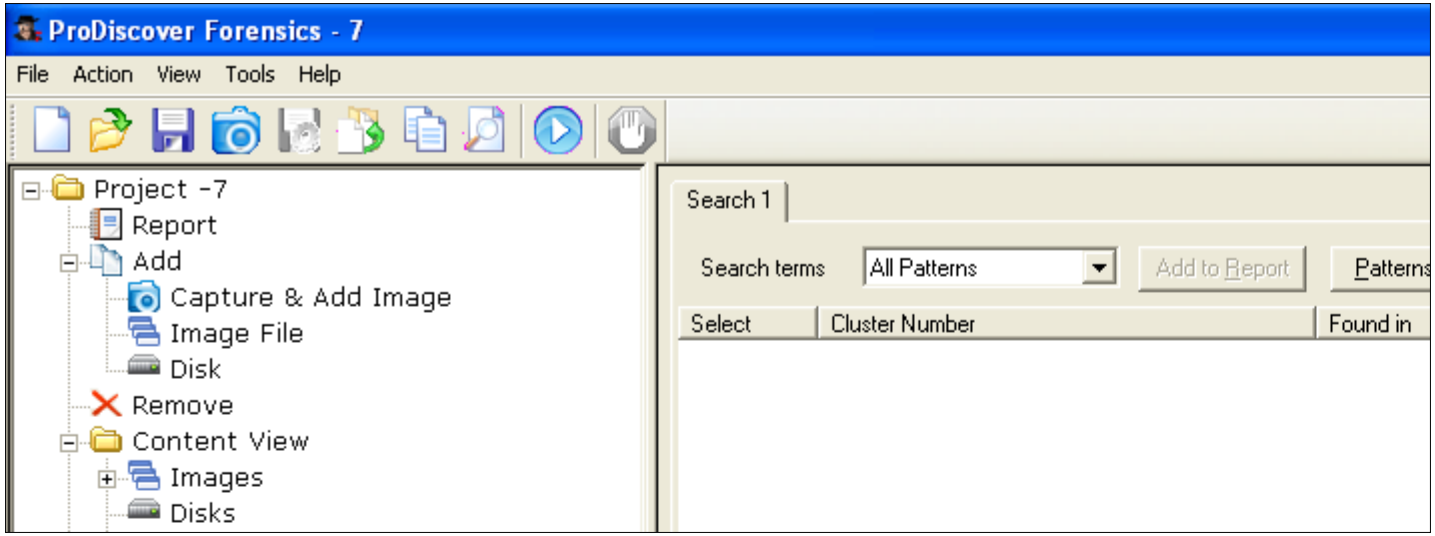
Windows Logon Passwords in RAM

Windows Login Password



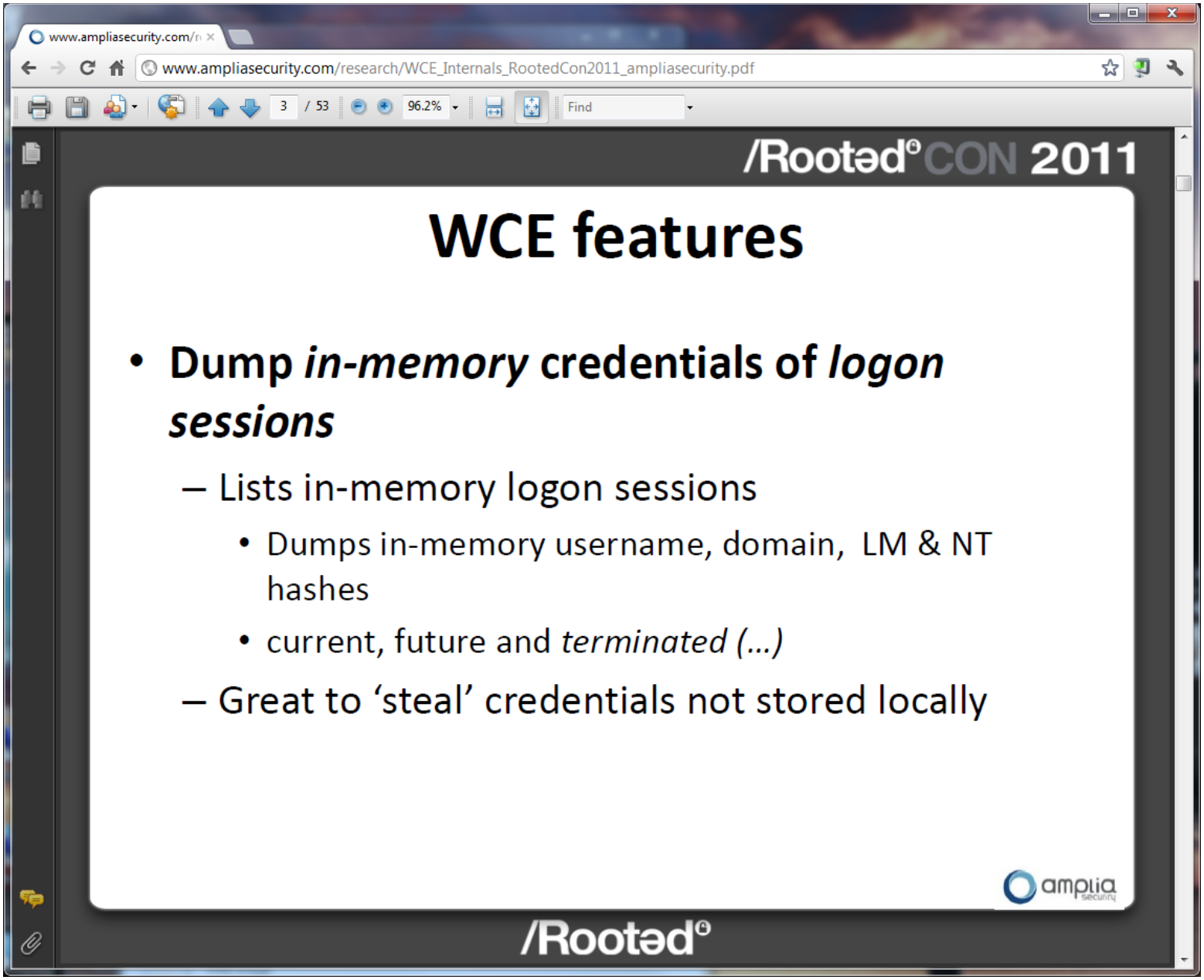
Not Found

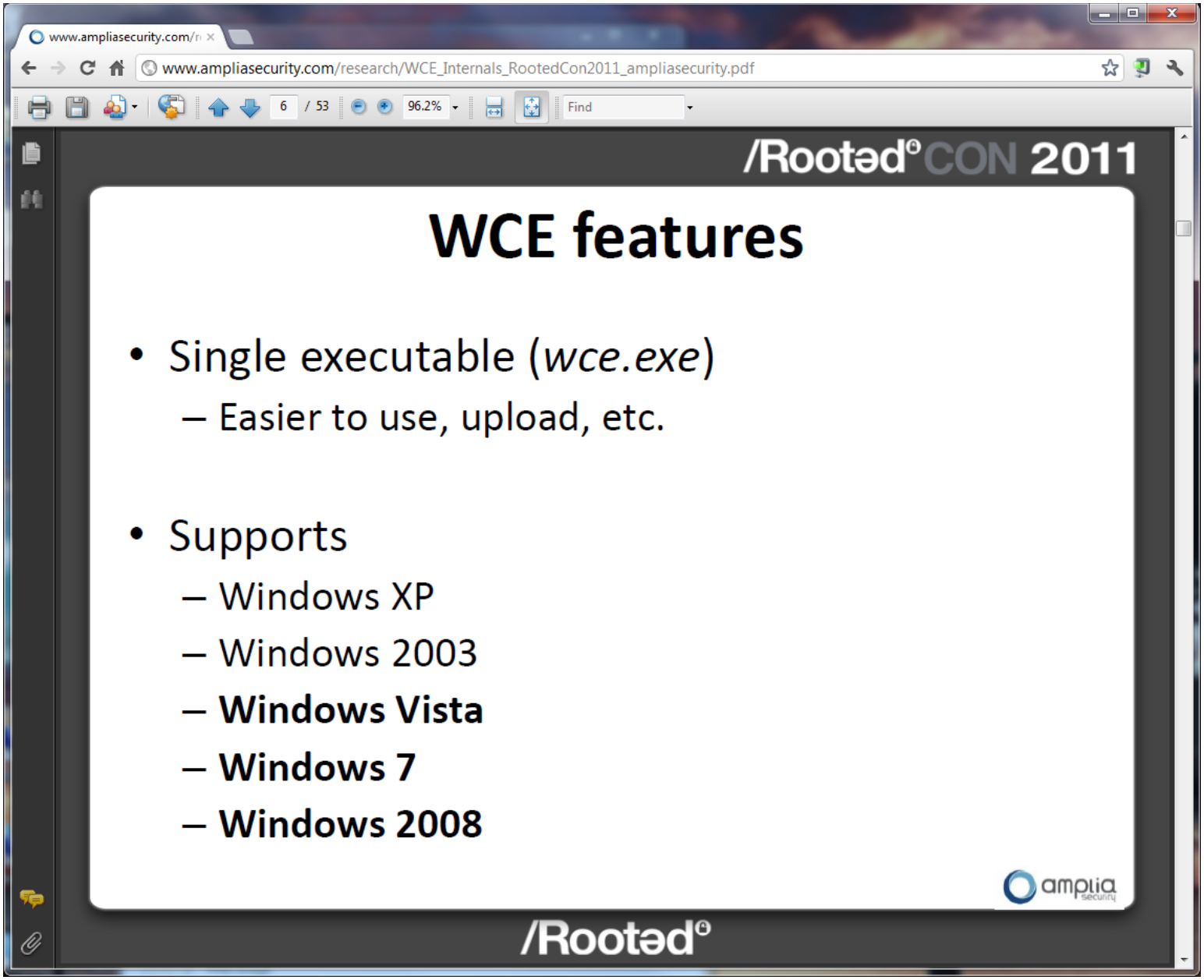
- Windows doesn't store login passwords in cleartext in RAM



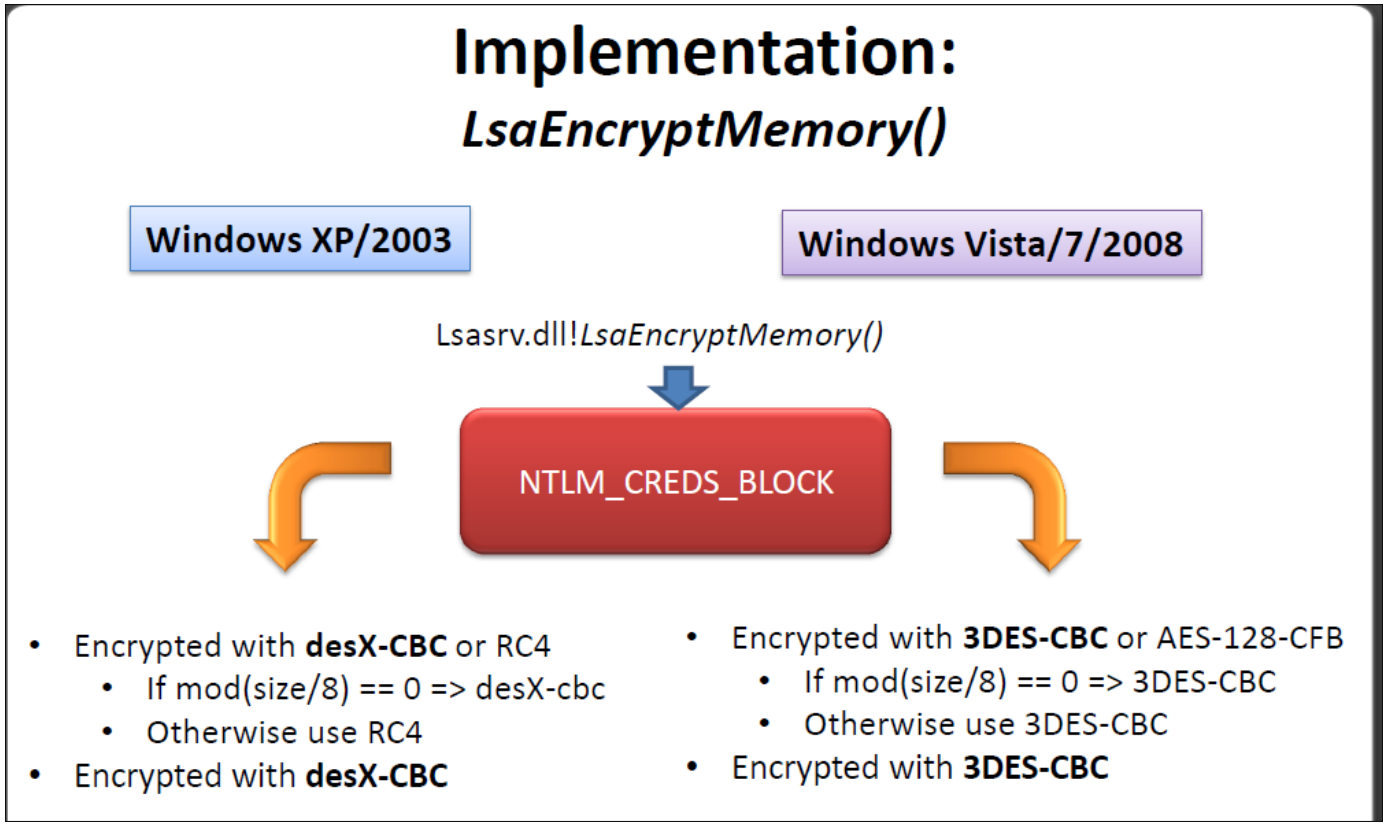
Windows Credential Editor

Written by Hernan Ochoa, 2011


www.ampliasecurity.com/
www.ampliasecurity.com/research/WCE_Internals_RootedCon2011_ampliasecurity.pdf
3 / 53
96.2%
Find
/RootedCON 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


www.ampliasecurity.com/
www.ampliasecurity.com/research/WCE_Internals_RootedCon2011_ampliasecurity.pdf
6 / 53
96.2%
Find
/RootedCON 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

Passwords are Encrypted



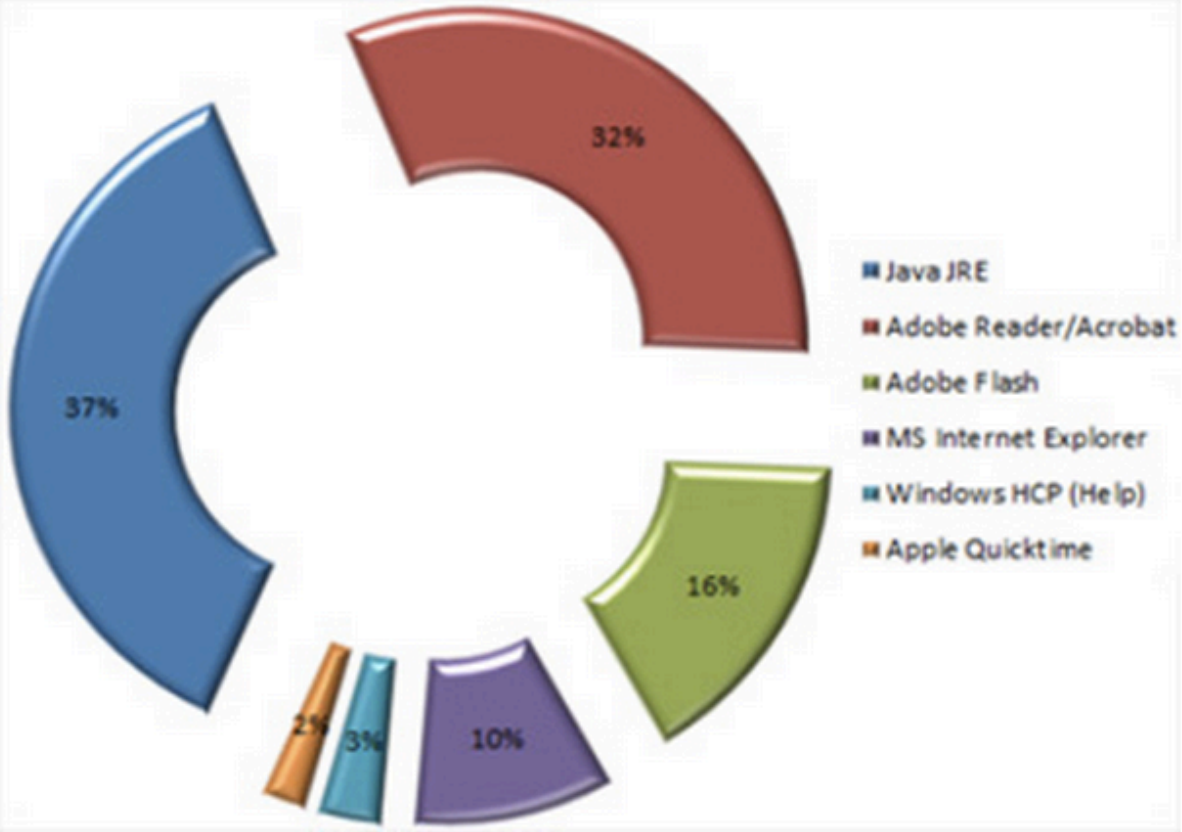
- But the Keys are in RAM

Java Attacks


www.net-security.org/malware_news.php?id=1863
This is how Windows get infected with malware
Posted on 05.10.2011
BOOKMARK
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:

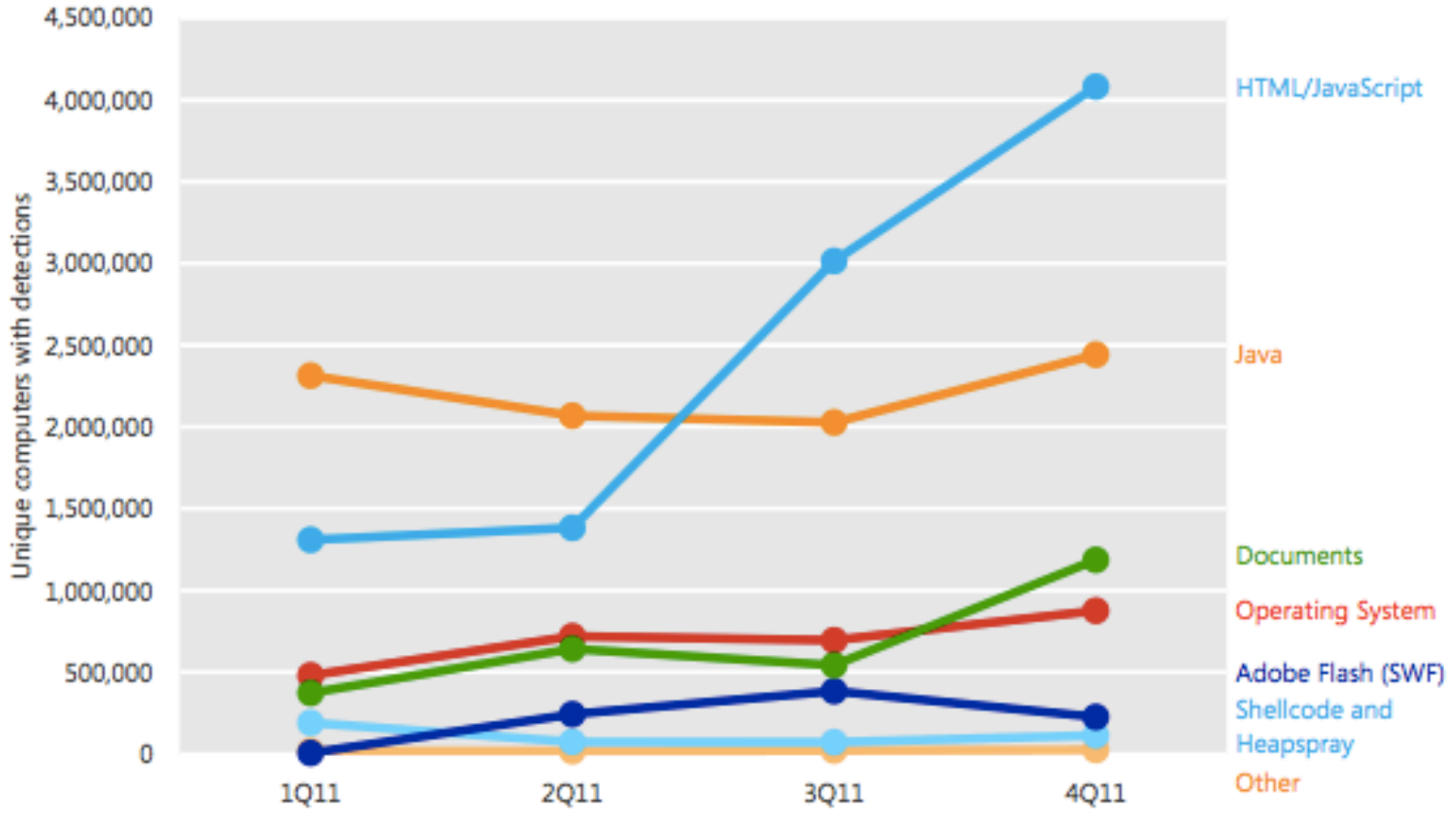


Microsoft Security Intelligence Report

Volume 12

July through December, 2011

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

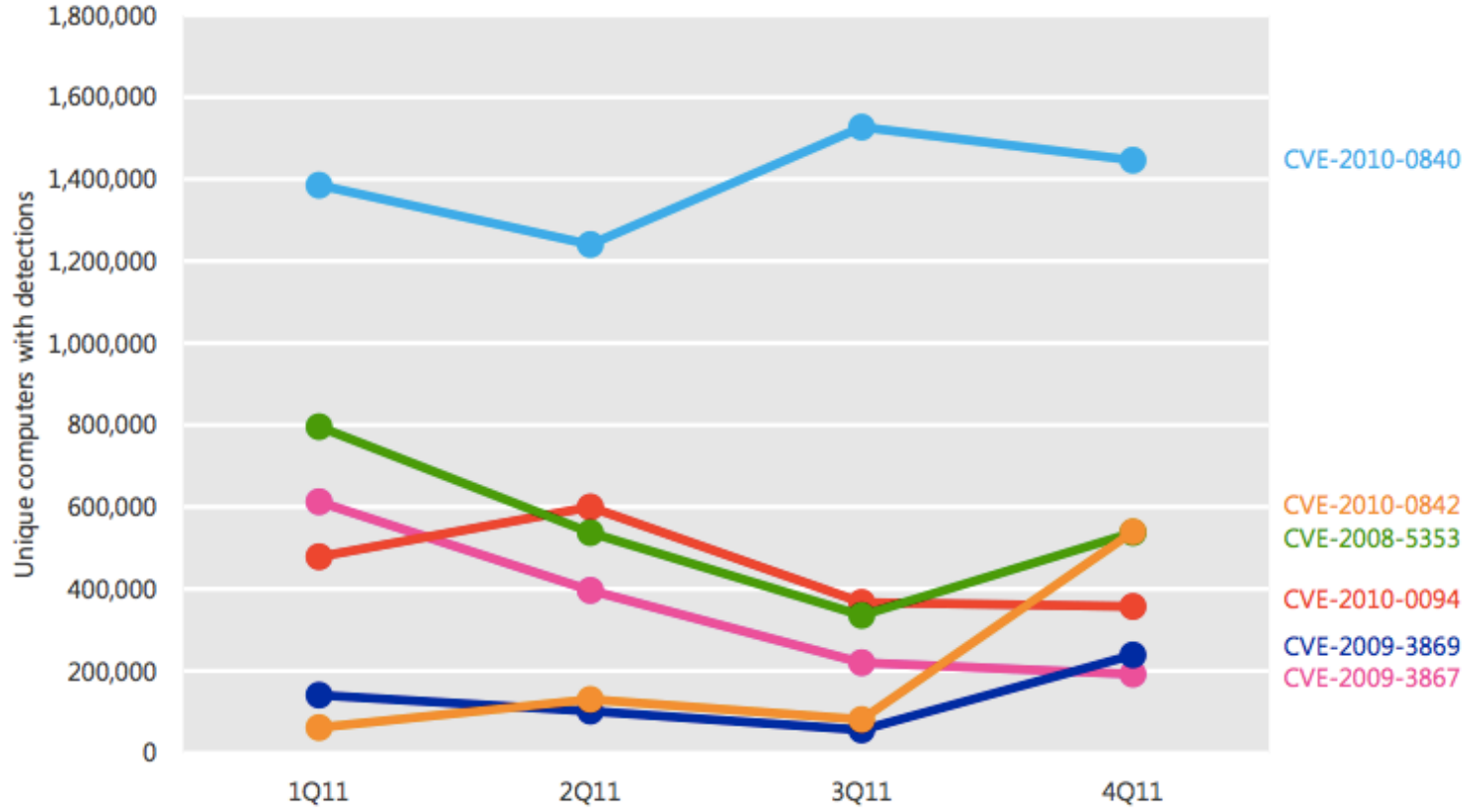


- The number of computers reporting exploits delivered through HTML or JavaScript increased steeply in the second half of 2011, due primarily to the emergence of JS/Blacole, a family of exploits used by the so-called "Blackhole" exploit kit to deliver malicious software through infected web pages.

Java Exploits

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

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

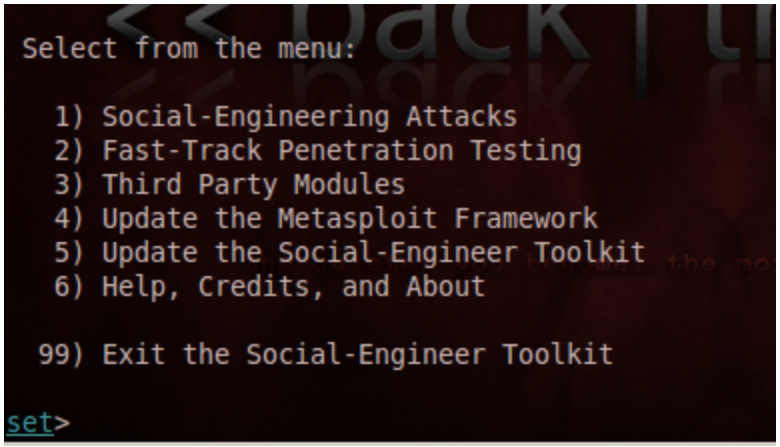


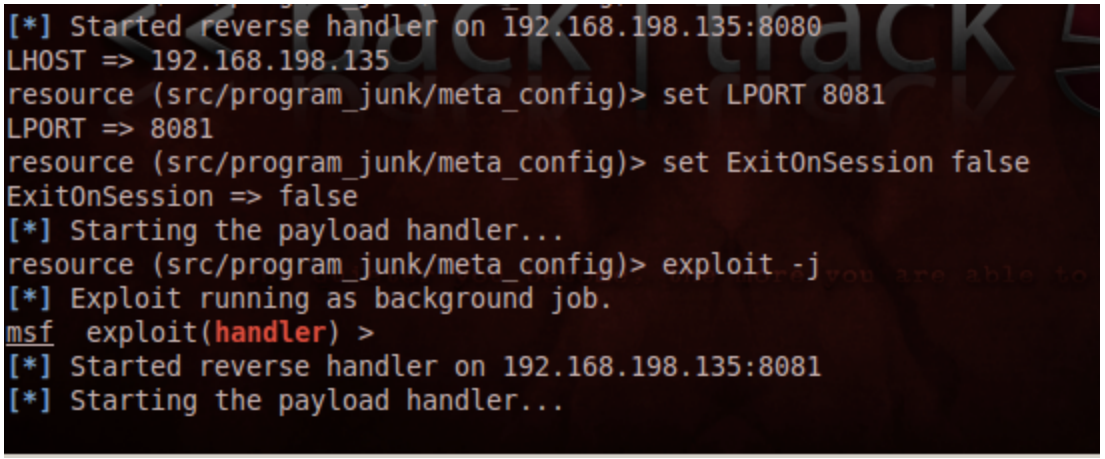
This Attack is Not Counted in Those Graphs

- 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

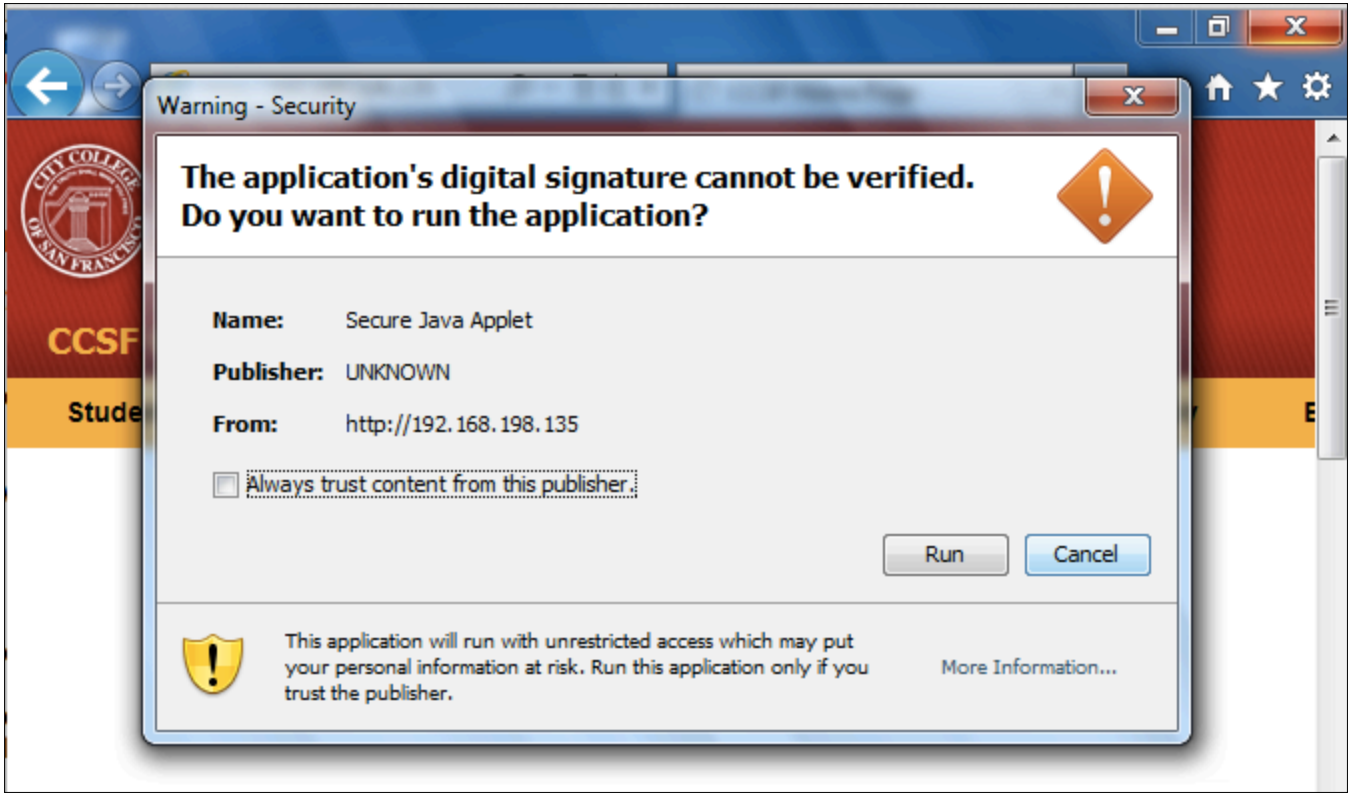
Social-Engineer Toolkit

- In BackTrack Linux

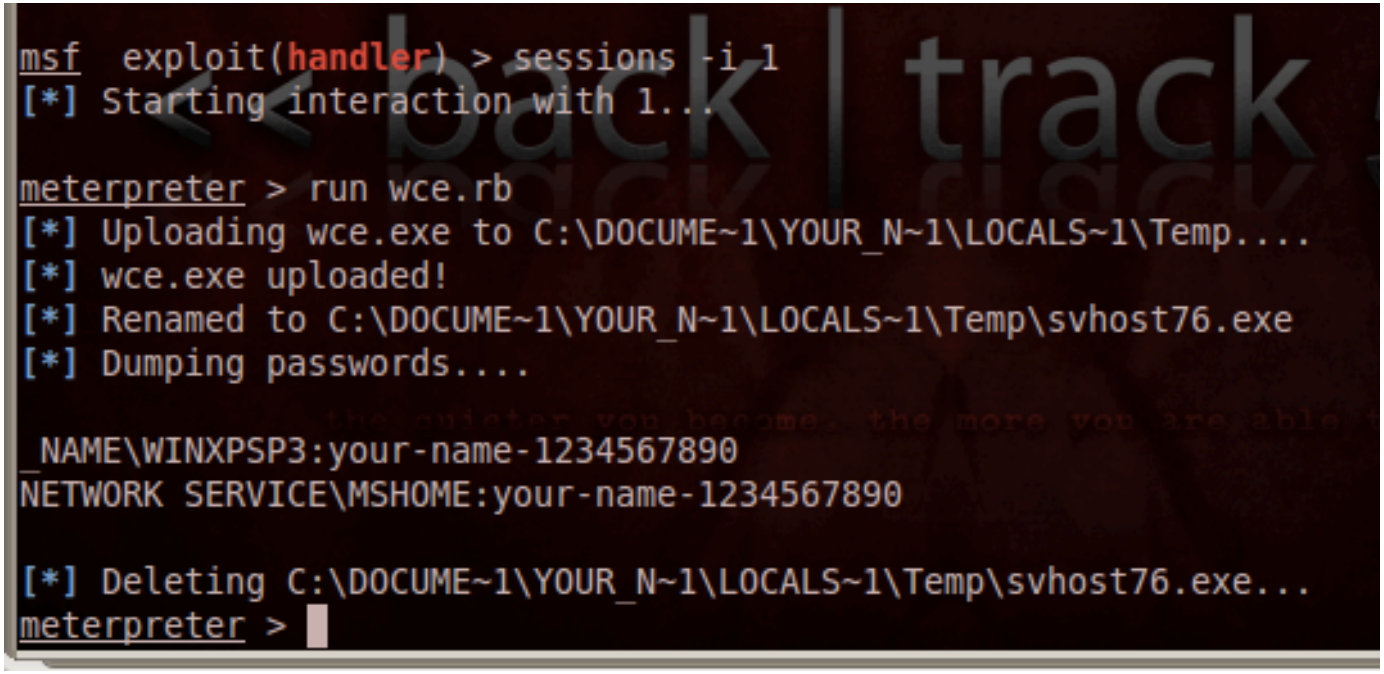




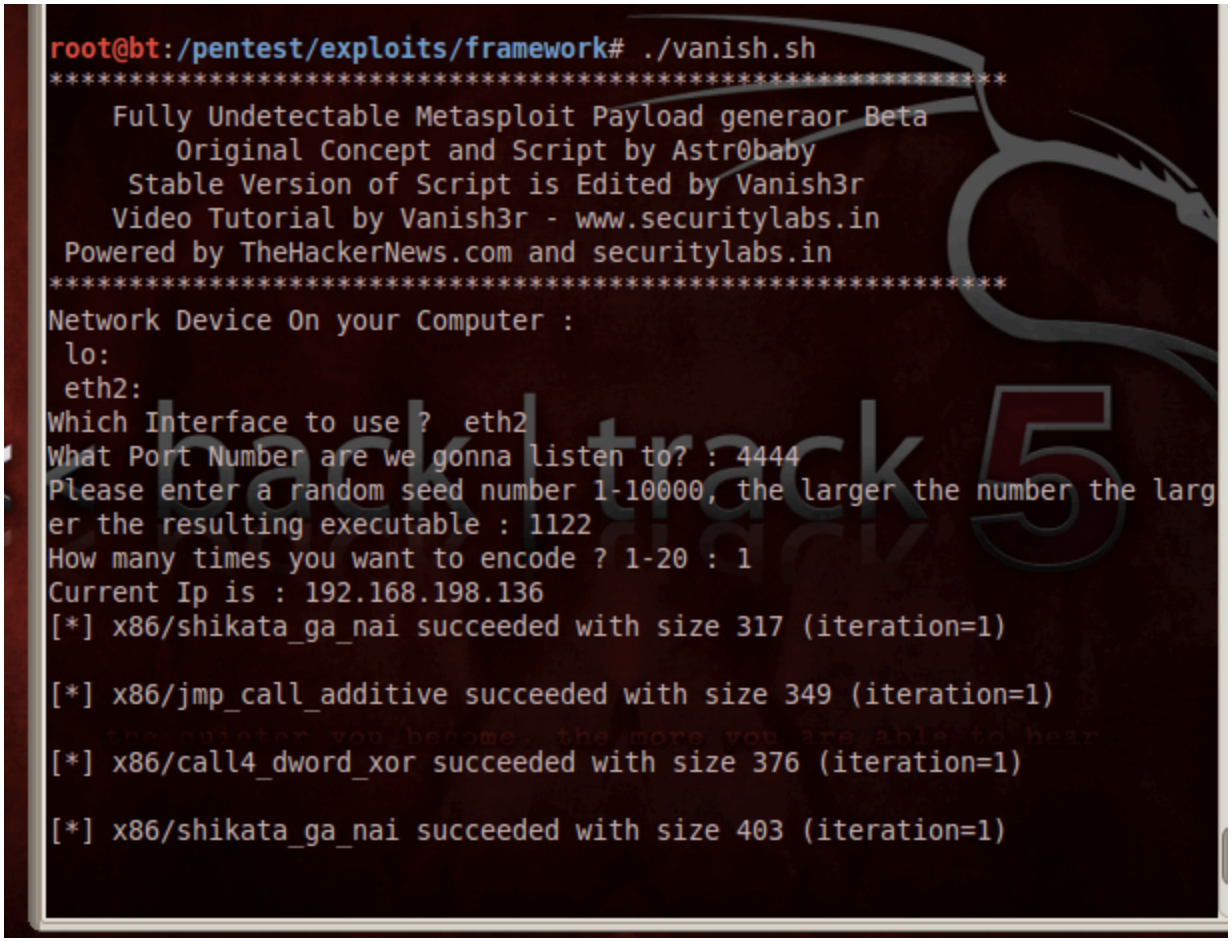
User Sees This Warning



Stolen Password!



Evading Antivirus

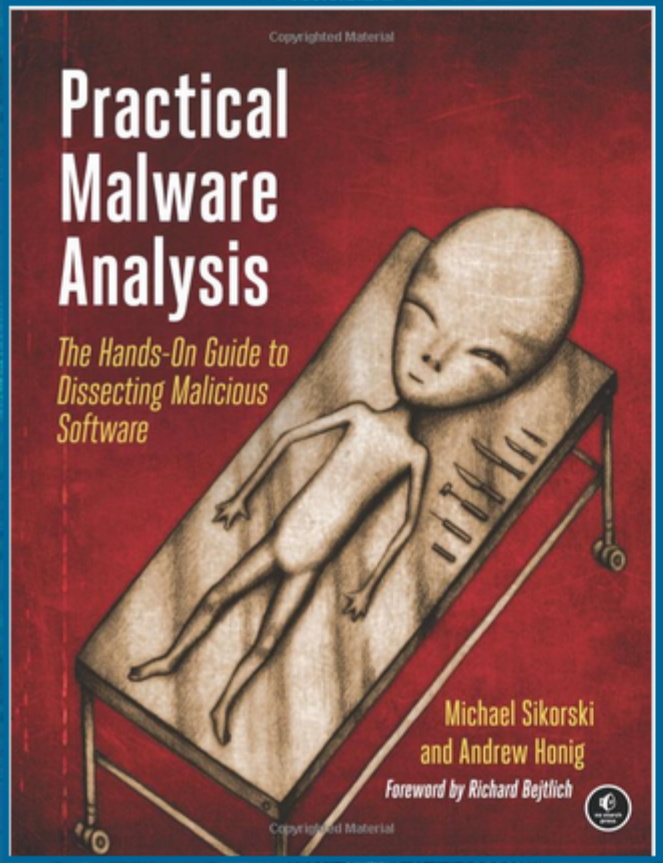


Effectiveness of AV Evasion

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

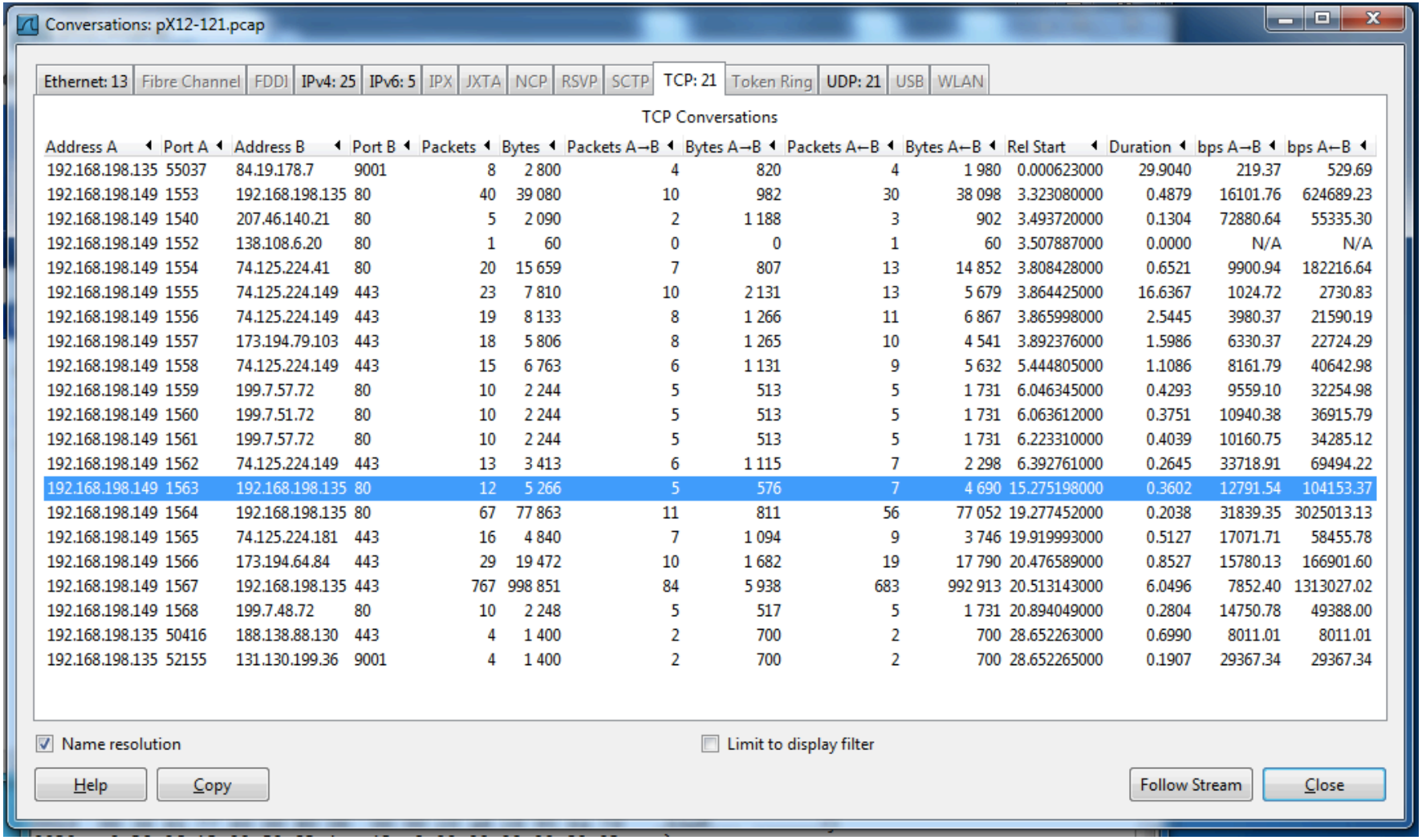
Links · Home Page

Techniques

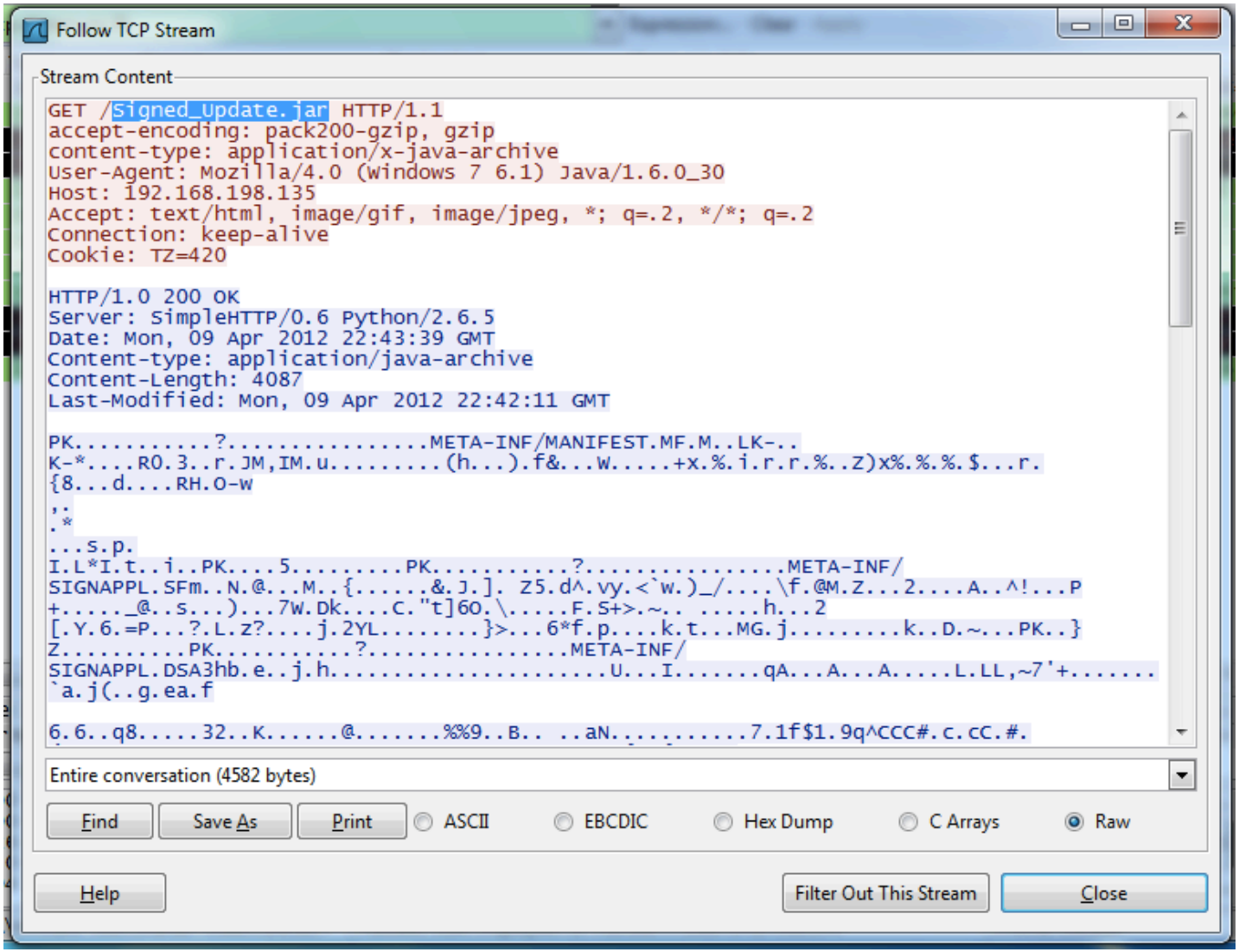
- Basic Static Analysis: File, Strings, and AV
- Basic Dynamic Analysis: RegShot, Wireshark, Process Monitor, LordPE
- Advanced Static Analysis: IDA Pro
- Advanced Dynamic Analysis: Debuggers (not included in this talk)

Basic Static Analysis

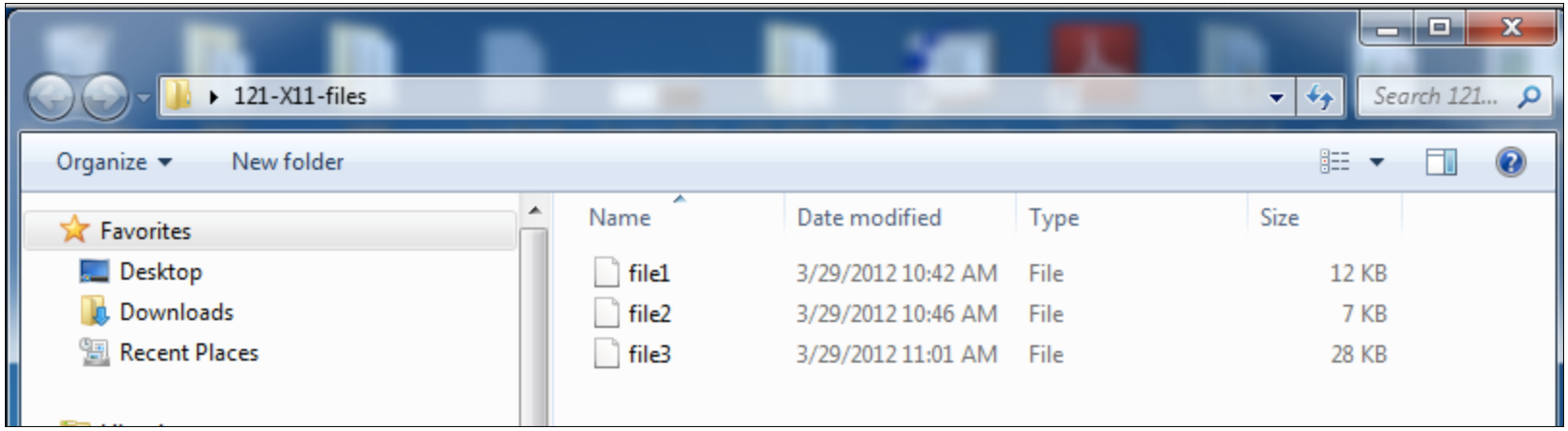
Harvesting Malware from Packet Captures with Wireshark



Save As


Follow TCP Stream
Stream Content
GET /Signed_Update.jar HTTP/1.1
accept-encoding: pack200-gzip, gzip
content-type: application/x-java-archive
User-Agent: Mozilla/4.0 (Windows 7 6.1) Java/1.6.0_30
Host: 192.168.198.135
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Cookie: TZ=420
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.6.5
Date: Mon, 09 Apr 2012 22:43:39 GMT
Content-type: application/java-archive
Content-Length: 4087
Last-Modified: Mon, 09 Apr 2012 22:42:11 GMT
PK..........?.............META-INF/MANIFEST.MF.M..LK-..
K-*....RO.3..r.JM,IM.u.....(h...).f&...W.....+x.%.i.r.r.%..Z)x%.%.%.$...r.
{8...d....RH.O-W
,:
.*
...s.p.
I.L*I.t..i..PK....5.....PK..........?.............META-INF/
SIGNAPPL.SFm..N.@...M..{.....&.J.]. Z5.d^.vy.<`w.)_/....\f.@M.Z...2....A..^!...P
+....._@..s...)...7W.Dk....C."t]6O.\.....F.S+>.~.. .....h...2
[.Y.6.=P...?.L.z?....j.2YL.....}>...6*f.p....k.t...MG.j.....k..D.~...PK..}
Z..........PK..........?.............META-INF/
SIGNAPPL.DSA3hb.e..j.h.....U...I.....qA...A...A.....L.LL,~7'+.....
`a.j(..g.ea.f
6.6..q8.....32..K.....@.....%%9..B.. ..aN.....7.1f$1.9q^CCC#.c.cC.#.
Entire conversation (4582 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

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

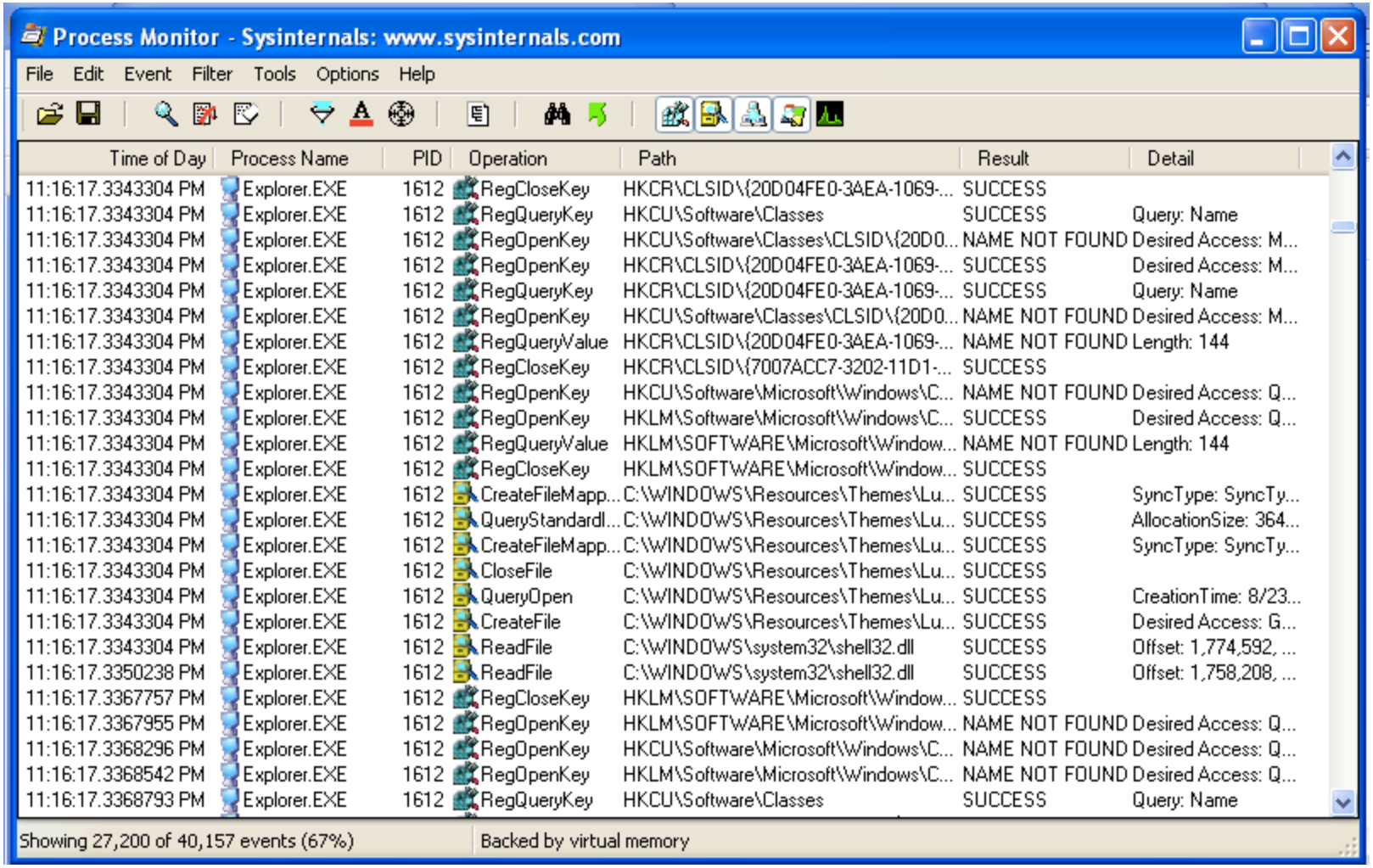
File Edit Format View Help

```
[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
Fyrrc
EryrnfrZhgrk
TrgYnfgReebe
PerngrZhgrkN
PerngrSvyrN
PybfrUnaqyr
xreary32.qyy
DSW
.com
rar
*.*
%c:\
[DSW]: Done with flood (%iKB/sec).
ddos.random
ddos.ack
```

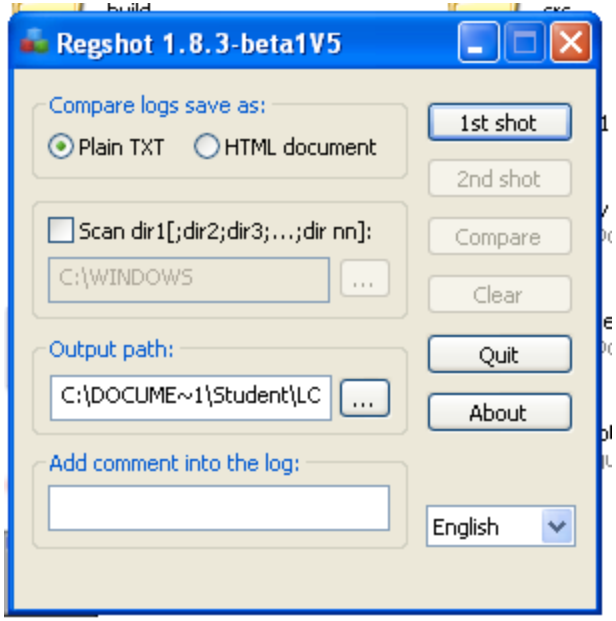
Basic Dynamic Analysis

Run Malware in a Virtual Machine

Process Monitor



RegShot


Regshot 1.8.3-beta1V5
Compare logs save as:
Plain TXT
HTML document
Scan dir1[;dir2;dir3;...;dir nn]:
C:\WINDOWS
Output path:
C:\DOCUME~1\Student\LC
Add comment into the log:
1st shot
2nd shot
Compare
Clear
Quit
About
English

RegShot Results

Deleted keys (0) for shot A

New keys (2) for shot B

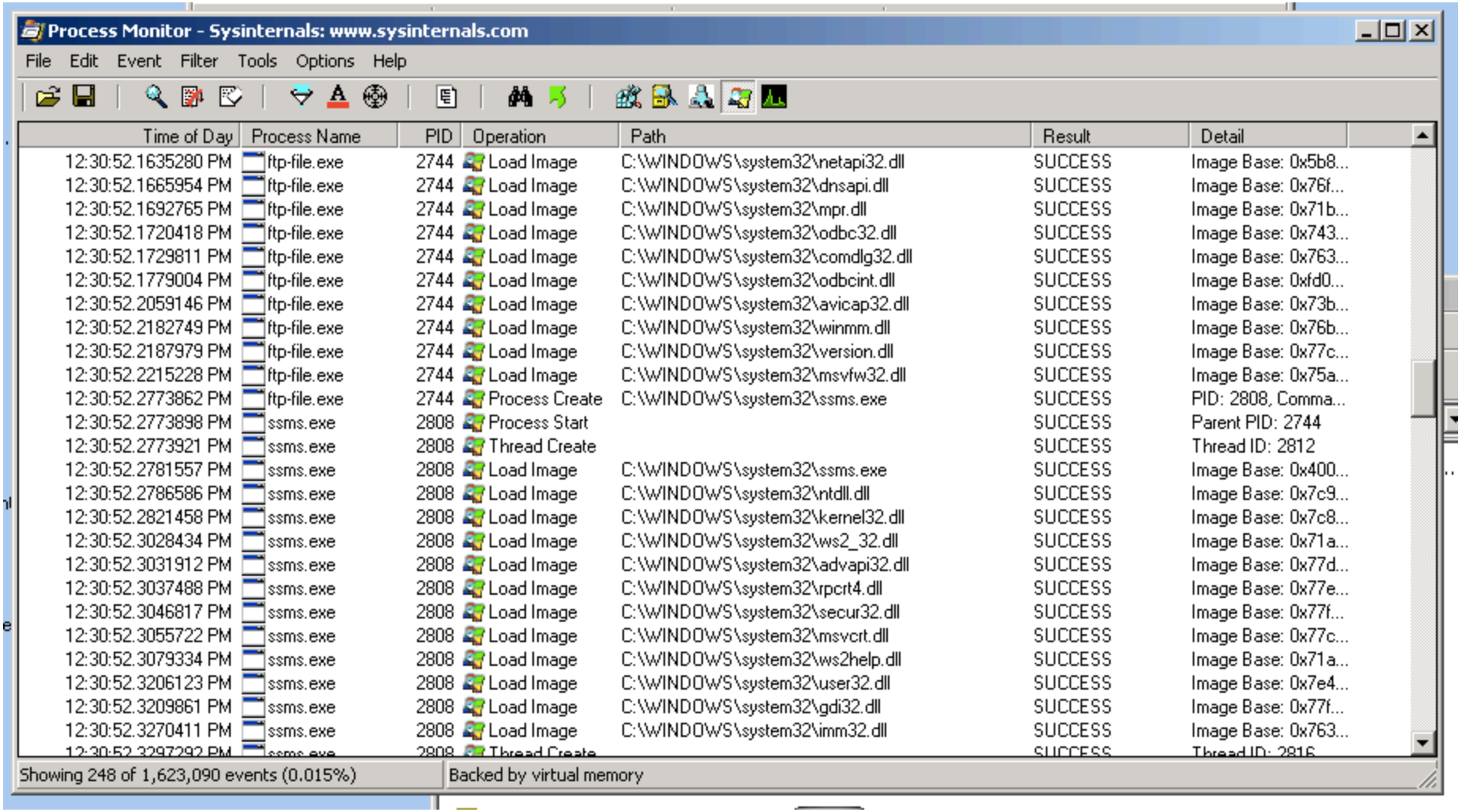
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_CURRENT_USER\Software\Microsoft\OLE]
```

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
```

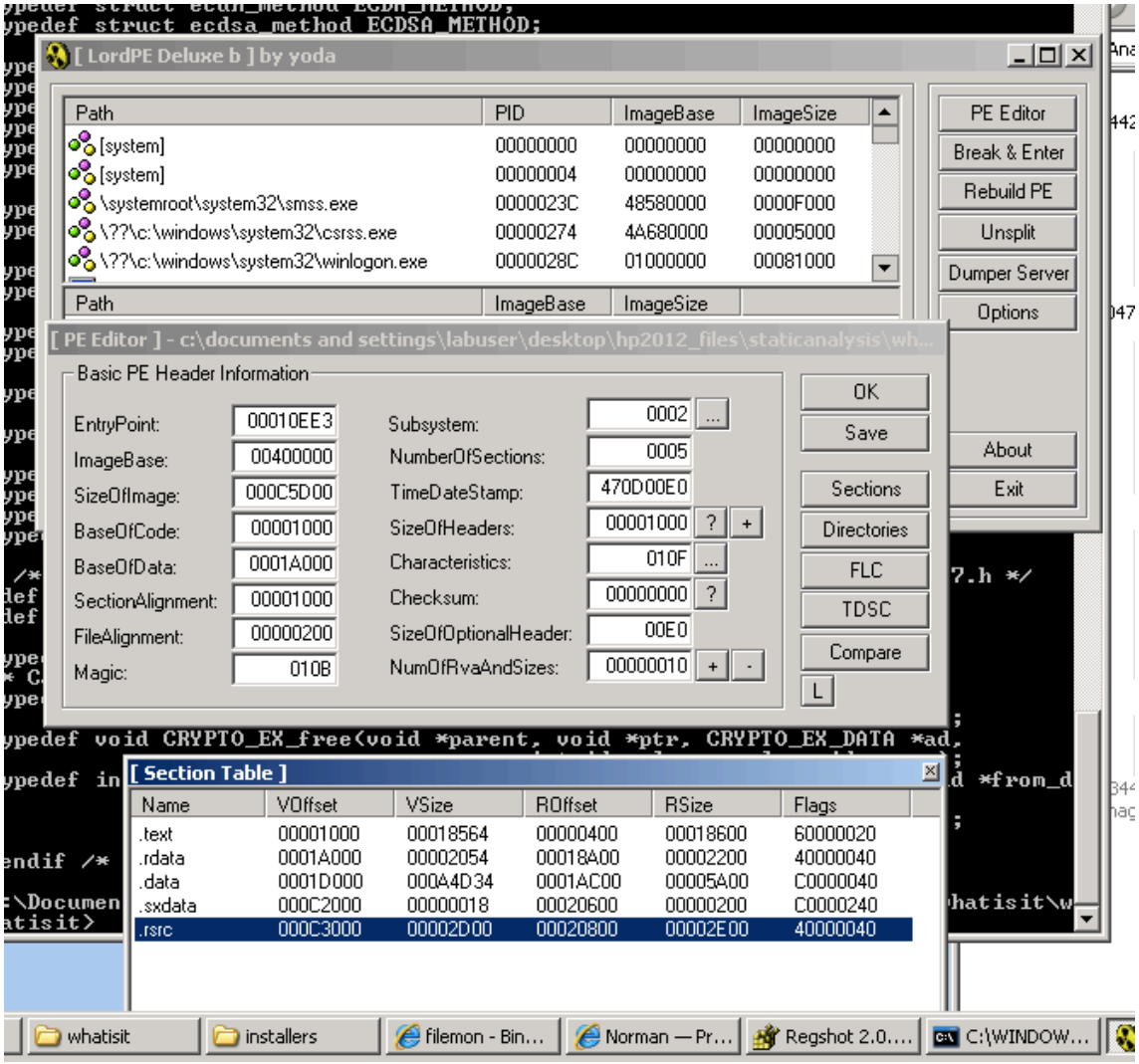
Process Monitor Results

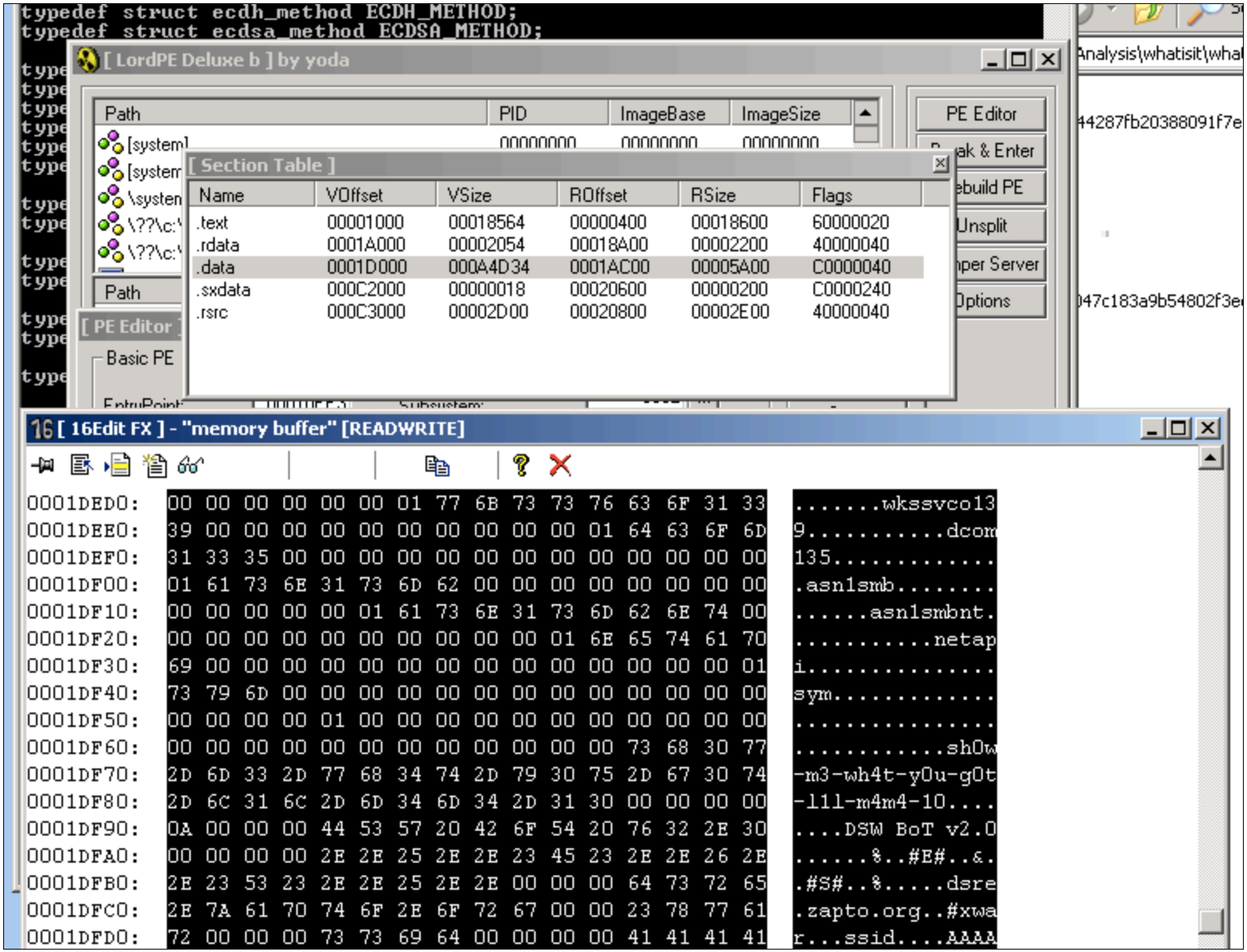


Packed Executables

- .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

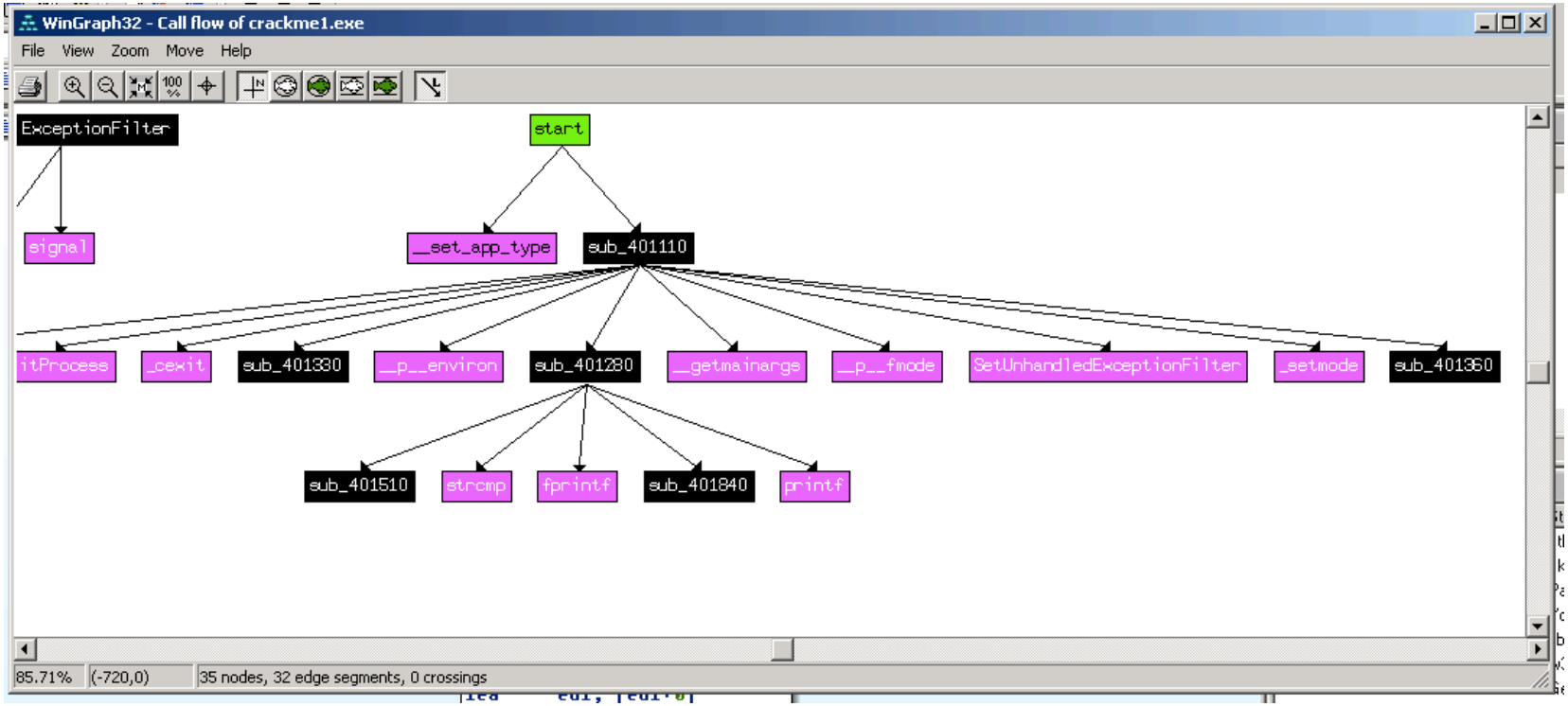

[LordPE Deluxe b] by yoda
Path
PID
ImageBase
ImageSize
[system] 00000000 00000000 00000000
[system] 00000004 00000000 00000000
\systemroot\system32\smss.exe 0000023C 48580000 0000F000
\??\c:\windows\system32\csrss.exe 00000274 4A680000 00005000
\??\c:\windows\system32\winlogon.exe 0000028C 01000000 00081000
PE Editor
Break & Enter
Rebuild PE
Unsplit
Dumper Server
Options
About
Exit
[PE Editor] - c:\documents and settings\labuser\desktop\hp2012_files\staticanalysis\wh...
Basic PE Header Information
EntryPoint: 00010EE3
ImageBase: 00400000
SizeOfImage: 000C5D00
BaseOfCode: 00001000
BaseOfData: 0001A000
SectionAlignment: 00001000
FileAlignment: 00000200
Magic: 010B
Subsystem: 0002
NumberOfSections: 0005
TimeDateStamp: 470D00E0
SizeOfHeaders: 00001000
Characteristics: 010F
Checksum: 00000000
SizeOfOptionalHeader: 00E0
NumOfRvaAndSizes: 00000010
OK
Save
Sections
Directories
FLC
TDSC
Compare
L
[Section Table]
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
whatisit
installers
filemon - Bin...
Norman — Pr...
Regshot 2.0....
C:\WINDOW...


typedef struct ecdh_method ECDH_METHOD;
typedef struct ecdsa_method ECDSA_METHOD;
[LordPE Deluxe b] by yoda
Path
PID
ImageBase
ImageSize
PE Editor
[Section Table]
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
[PE Editor]
Basic PE
Unsplit
Options
Analysis\whatisit\what
44287fb20388091f7e
047c183a9b54802f3e
16 [16Edit FX] - "memory buffer" [READWRITE]
0001DED0: 00 00 00 00 00 00 01 77 6B 73 73 76 63 6F 31 33 ....wkssvco13
0001DEE0: 39 00 00 00 00 00 00 00 00 00 00 01 64 63 6F 6D 9...........dcom
0001DEF0: 31 33 35 00 00 00 00 00 00 00 00 00 00 00 00 00 135.............
0001DF00: 01 61 73 6E 31 73 6D 62 00 00 00 00 00 00 00 00 .asn1smb........
0001DF10: 00 00 00 00 00 01 61 73 6E 31 73 6D 62 6E 74 00 ......asn1smbnt.
0001DF20: 00 00 00 00 00 00 00 00 00 00 01 6E 65 74 61 70 ....netap
0001DF30: 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 i...............
0001DF40: 73 79 6D 00 00 00 00 00 00 00 00 00 00 00 00 00 sym.............
0001DF50: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 ....
0001DF60: 00 00 00 00 00 00 00 00 00 00 00 00 73 68 30 77 ....sh0w
0001DF70: 2D 6D 33 2D 77 68 34 74 2D 79 30 75 2D 67 30 74 -m3-wh4t-y0u-g0t
0001DF80: 2D 6C 31 6C 2D 6D 34 6D 34 2D 31 30 00 00 00 00 -l1l-m4m4-10....
0001DF90: 0A 00 00 00 44 53 57 20 42 6F 54 20 76 32 2E 30 ....DSW BoT v2.0
0001DFA0: 00 00 00 00 2E 2E 25 2E 2E 23 45 23 2E 2E 26 2E ......%..#E#..&.
0001DFB0: 2E 23 53 23 2E 2E 25 2E 2E 00 00 00 64 73 72 65 .#S#..%.....dsre
0001DFC0: 2E 7A 61 70 74 6F 2E 6F 72 67 00 00 23 78 77 61 .zapto.org..#xwa
0001DFD0: 72 00 00 00 73 73 69 64 00 00 00 00 41 41 41 41 r...ssid....AAAA

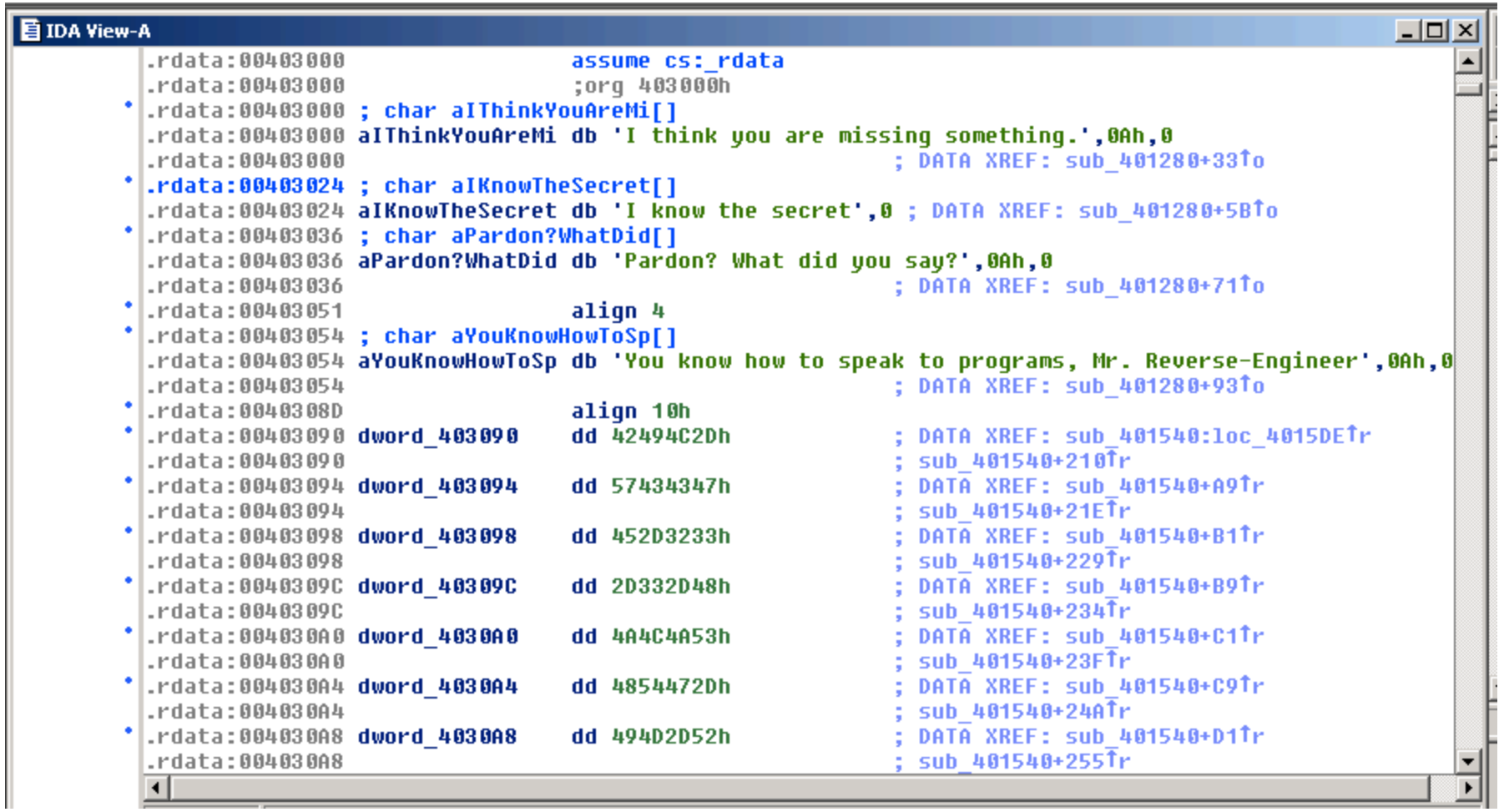
Advanced Static Analysis

IDA Pro

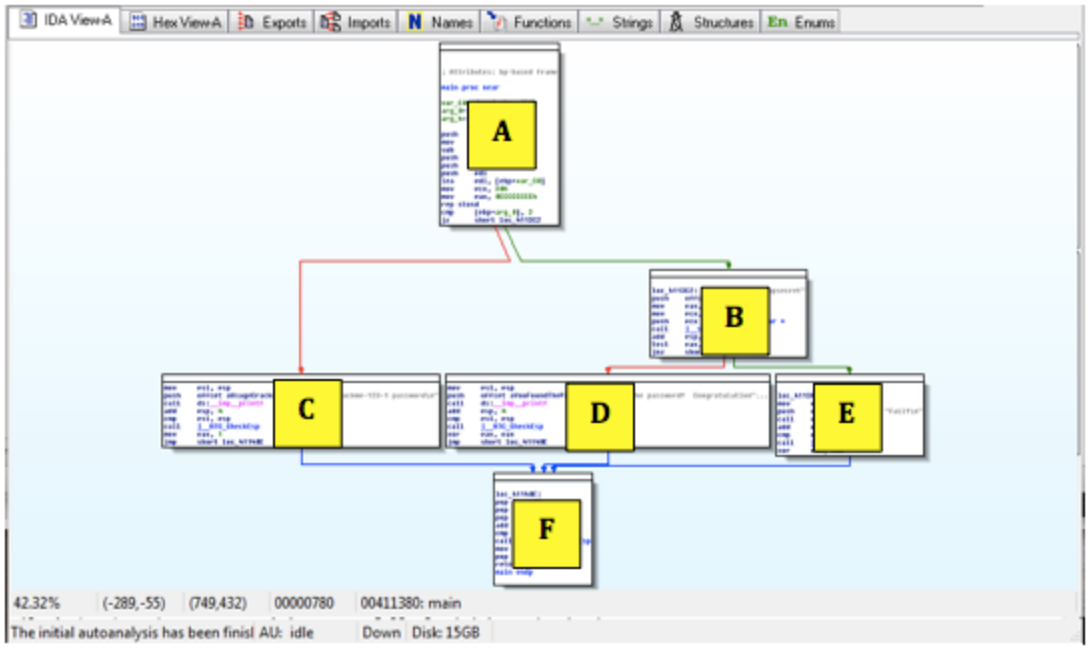
Disassembler



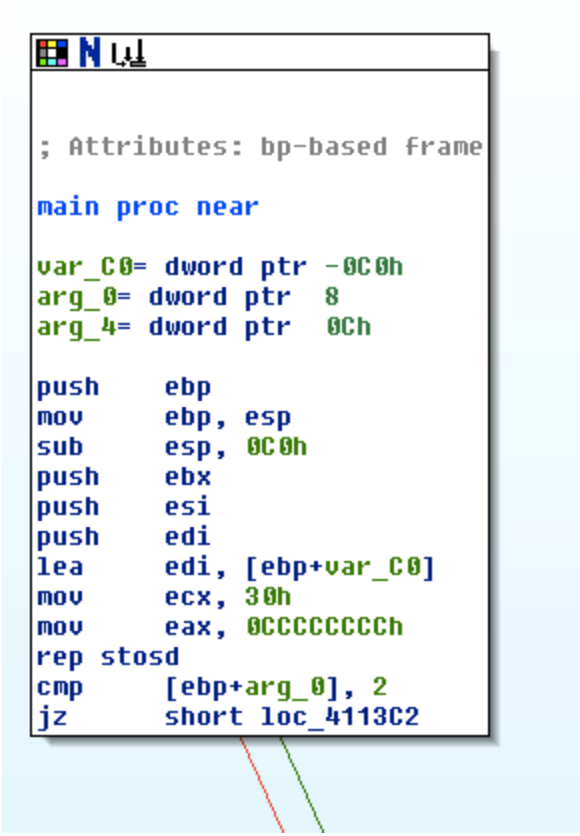
Mind-Boggling Complexity



Skip Details

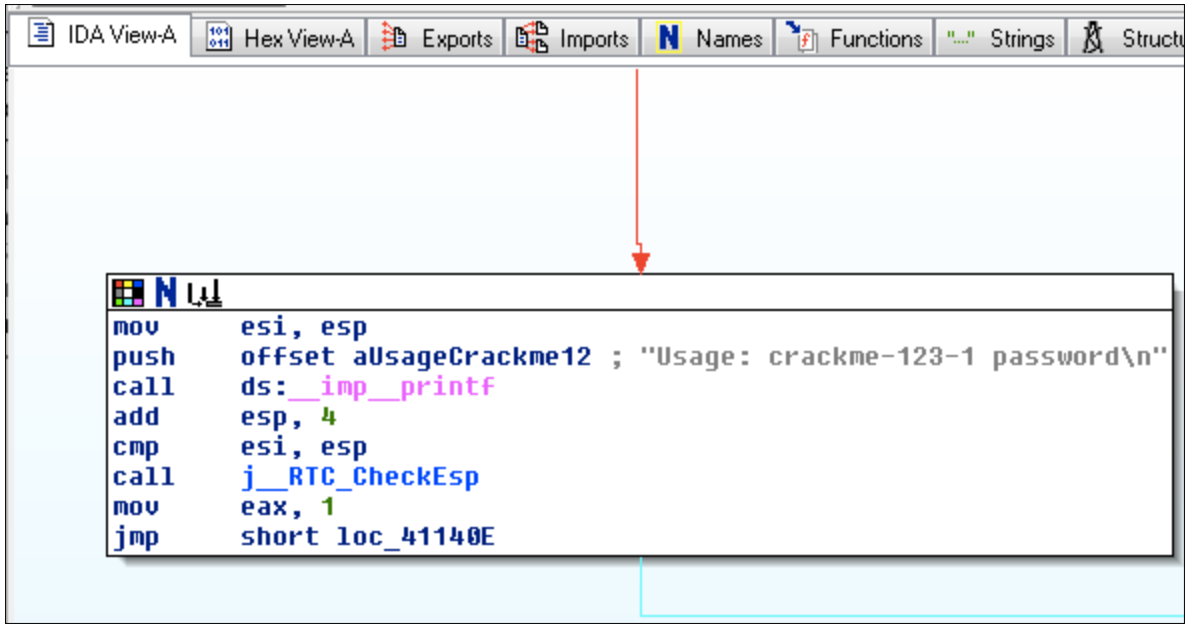


Module A: Compare, Jump

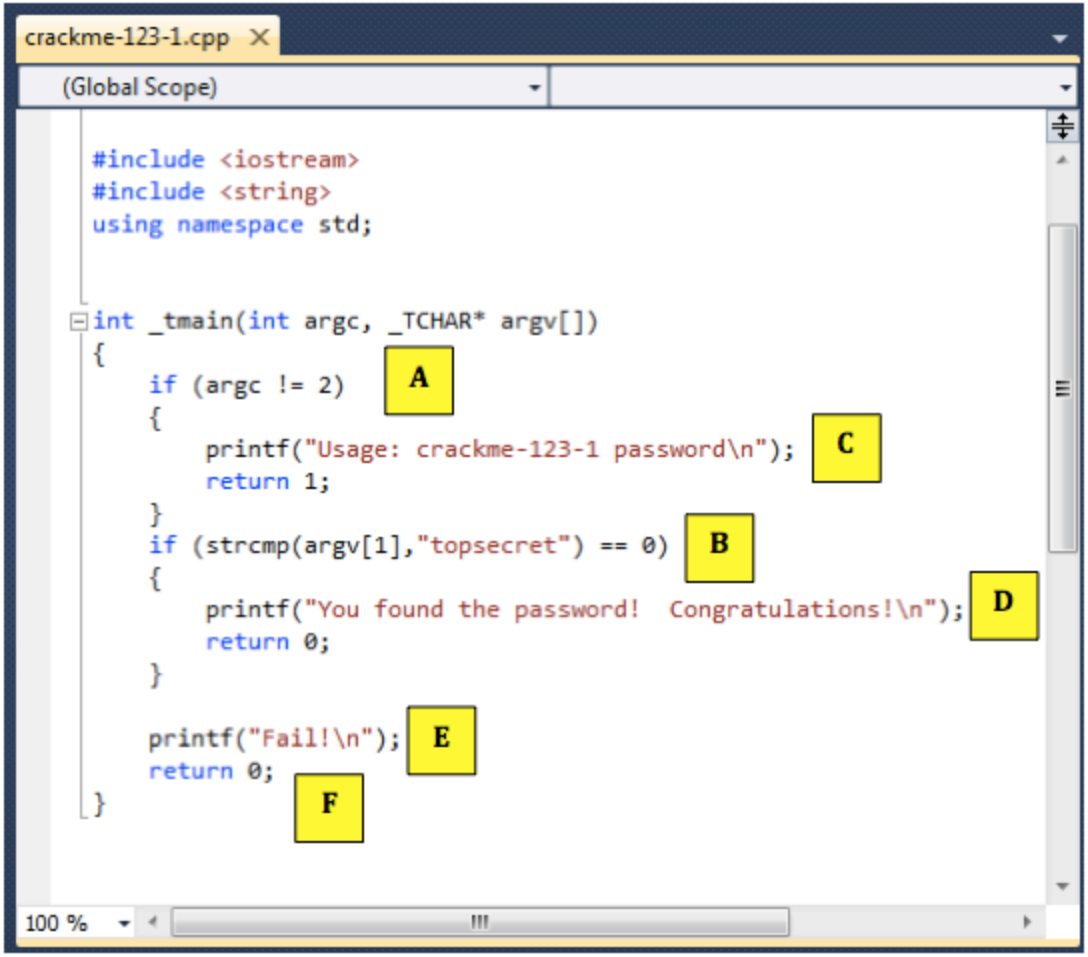


```
; Attributes: bp-based frame

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
```

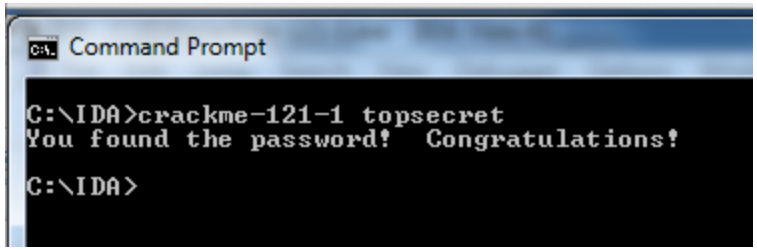
Module C: Usage Instructions



C Source Code



Solution


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