

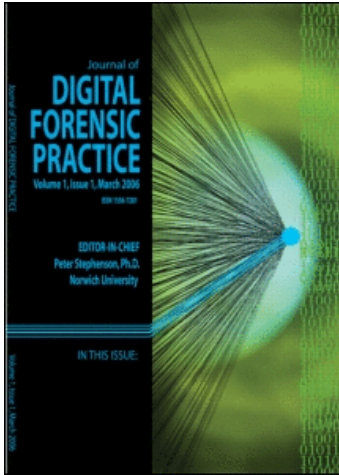
This article was downloaded by:

On: 23 November 2009

Access details: *Access Details: Free Access*

Publisher *Taylor & Francis*

Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



## Journal of Digital Forensic Practice

Publication details, including instructions for authors and subscription information:

<http://www.informaworld.com/smpp/title~content=t716100764>

### Battling Anti-Forensics: Beating the U3 Stick

Thijs Bosschert <sup>a</sup>

<sup>a</sup> Fox-IT, The Netherlands

**To cite this Article** Bosschert, Thijs 'Battling Anti-Forensics: Beating the U3 Stick', Journal of Digital Forensic Practice, 1: 4, 265 – 273

**To link to this Article:** DOI: 10.1080/15567280701417975

**URL:** <http://dx.doi.org/10.1080/15567280701417975>

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: <http://www.informaworld.com/terms-and-conditions-of-access.pdf>

This article may be used for research, teaching and private study purposes. Any substantial or systematic reproduction, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.

ARTICLE

# Battling Anti-Forensics: Beating the U3 Stick

**Thijs Bosschert**

Fox-IT, P.O. Box 638, 2600 AP  
Delft, The Netherlands

---

**ABSTRACT** With the growing knowledge of digital forensics there is also a growing knowledge in the field of anti-forensics. More software and products see the light each day, which can make digital forensic investigations more difficult to do. One new product in the world of anti-forensics is a USB stick, which can be used to take your favorite programs and files with you on the road. You can use them on any computer and leave no traces of what you have been doing on the computer. Besides being useful for a lot of people, the features of this stick can also be abused. Offences like hacking, fraud, spamming, and the like could be harder to investigate if no traces of the offense are to be found on the computer because one of these USB sticks has been used. This article is about the U3 USB stick; it offers you the opportunity to travel with your files and programs, but does it indeed leave no traces?

**KEYWORDS** anti-forensics, U3 stick, USB stick, digital forensics, slack space, free space

---

## U3 IN THE PRESS

The U3 stick has had a lot of press coverage, below are a couple of quotes from the press, which show the general thoughts about the U3 stick.

### U3 Website

Private and protected computing

*The U3 platform is designed to leave no trace of the user's data or application usage on the host computer after the smart drive is removed.* The U3 platform also supports the creation of security solutions to protect the privacy and security of user data and applications. These solutions include encrypted files and folders, and sign-on and password protection and management [1].

### The Inquirer

On the plus side, it makes perfect sense for end users. Effectively you can carry all your favourite programs and software settings around on a single USB memory card. *Plug it in and off you go. Tug it out again and there's no trace of your data left on the host PC [2].*

---

Thijs Bosschert is working as a forensic IT expert at Fox-IT in Delft, The Netherlands. Besides doing forensics investigations he also works on audit projects as well as research projects. He is a CISSP associate and holds the private investigator certification.

## PC World

They're great for security purposes, too; plug your U3 drive into some other machine and you can use a Web browser or e-mail program on it *without leaving your footprints* in the other machine's cookies and history files [3].

## Tweakers.net

The ability to take your important software and files with you, to use them on the road *without leaving traces on the computer you use*, is very useful.

[Het kunnen meedragen van belangrijke software en bestanden, om ze bijvoorbeeld op reis te gebruiken *zonder sporen achter te laten op de computer waar je achter werkt*, is erg praktisch.]<sup>1</sup> [4].

## Computer Idee

Imagine that you can save all your software and files on a usb-stick and use them on any computer, *without leaving traces on that computer* . . . without putting files on the harddisk of the computer or making changes in the registry.

[Stel dat u al uw software en documenten kon opslaan op een usb-stick en er op iedere willekeurige pc mee kon werken. *Zonder op die computer sporen na te laten* bovendien...zonder bestanden op de harde schijf van de pc te zetten of wijzigingen in het register aan te brengen.]<sup>2</sup> [5].

## RESEARCH SETUP

### The U3 Stick

In this article we use the term "U3 stick," which combines the hardware of the USB stick and the software of U3. The U3 stick we tested was an "Intuix S300 512 MB USB 2.0 high speed" USB stick. The applications that were pre-installed on this U3 stick were removed after an initial test.

To use your favorite applications on the U3 stick, you can install them using the application on the U3 stick itself or by downloading them from the web site. The following applications have been installed by us on the U3 stick we tested.

- Office applications
  - Open Office (version 2.0.1.0)
- Internet applications
  - WeatherBug (version 1.0.0.8)
  - Firefox (version YourBrainz 1.5.0.2)
  - Maxthon Browser (version 1.5.2)
  - FileZilla (version 2.22)

- Trillian (version 3.11)
- Media applications
  - Irfanview (version 3.9.8.1)
  - WinAmp (version 5.1.1.0)
- Games
  - Electric Eddie (version 1.1.1.0)
  - Party Poker (version 1.0.0.1)
- Other applications
  - MedicAlert (version not defined)
  - Winrar (version 3.5.1.4)

## Testing Environment

The U3 stick has been tested on a fully patched (at the time of testing) Windows XP (SP2) installation. To see all the changes the U3 stick tries to make on the hard disk, no restrictions were made to the user profile that was used to test the U3 stick. None of the applications installed on the U3 stick were locally installed on the computer we used for the testing.

## Actions

To investigate whether the U3 stick leaves any traces behind after it has been used, the U3 stick was plugged into a computer and all the applications were used for a short while. Afterwards the U3 stick was ejected using the eject option in the U3 menu.

## RESULTS

After the U3 stick was used, we did a forensic investigation to see whether we could find any traces on the computer the U3 stick had been used on. We did indeed find traces. This chapter discusses the most important traces that were found; not every trace that has been found will be named.

## U3Launcher.log

With each launch of the U3Launcher application (the program that starts from the U3 stick and shows the links to the U3 applications) the U3 stick writes information to a log file. This log file can be found in C:\Documents and Settings\3 with <username> being the username of the user using the U3 stick and has the name

U3Launcher.log. In this file the U3Launcher writes information about the U3Launcher application; this information includes when the U3Launcher application was started, which drives the U3 stick has used, and what the serial number of the U3 stick is. This information can be used to find out when and which U3 stick has been used on a computer. The C:\Documents and Settings\\Local Settings\Temp\U3Launcher.log file is not removed from the computer after the U3 stick has been ejected. An example of a U3launcher.log file is shown in Figure 1. This example contains one connection of a U3 stick to the computer.

## Directories

When the U3 stick is used on a computer it makes its own directory in the following place: C:\Documents and Settings\\Application Data\U3\. One of the first traces to look for that makes it likely that a U3 stick has been used on a computer can be this U3 directory. In the U3 directory there is another directory, one that seems to have a random name. We found that the directory name is the serial number of the U3 stick, which can also be found in the U3Launcher.log file (see U3Launcher.log).

The directory name in our test setup was “0D30CC50B0508885” (C:\Documents and Settings\\Application Data\U3\0D30CC50B0

508885). While in use, the U3 stick appears to make new directories within the random directory. The new directories also seem to have a random name for each application they stand for; the names of the application directories are the same as on the U3 stick (U3:\System\Apps\). A couple of directories we stumbled upon are listed in Figure 2; the applications they belong to are listed behind them.

Inside each application directory we found the directory *Manifest*. The directory *Manifest* usually contains two files, an icon file for the program that the directory is for and a Manifest.u3i file. The Manifest.u3i file shows us exactly which program the directory has been made for; it also shows us which icon it uses, the version of the software, the vendor of the software, the description of the software, etc.

So with the information in the Manifest files (C:\Documents and Settings\\Application Data\U3\\\Manifest\Manifest.u3i) we can see which programs on the U3 stick have been used on the computer. An example Manifest.u3i file is shown Figure 3. This Manifest.u3i file contains the information about the U3 game Electric Eddie. The application uuid is the same as the name of the directory this file has been found in.

```
***[H:\LaunchU3.exe]*** info: LastError=[0] [3872 - 5764] [31/08/2006
11:01:00.581] U3Launcher started
***[H:\LaunchU3.exe]*** info: LastError=[0] [3872 - 364] [31/08/2006
11:01:00.591] U3Launcher TerminateProcessProc starting
***[H:\LaunchU3.exe]*** error: LastError=[0] [3872 - 5764] [31/08/2006
11:01:00.721] SERIAL 0D30CC50B0508885
***[H:\LaunchU3.exe]*** error: LastError=[0] [3872 - 5764] [31/08/2006
11:01:00.761] CAutoPlayMgr::Initialize
***[H:\LaunchU3.exe]*** info: LastError=[0] [3872 - 5764] [31/08/2006
11:01:00.771] U3Launcher started from U3 device
***[H:\LaunchU3.exe]*** info: LastError=[0] [3872 - 5764] [31/08/2006
11:01:00.781] U3DeviceInfo Serial:0D30CC50B0508885
DevCaps:DEVCAPS_REMOVABLE & DEVCAPS_CDROM
CD Path:G
Removable:H
***[H:\LaunchU3.exe]*** info: LastError=[0] [3872 - 5764] [31/08/2006
11:01:02.299] RunLaunchPad [C:\Documents and Settings\username\Application
Data\U3\0D30CC50B0508885\LaunchPad.exe -serial=0D30CC50B0508885 -
drives=Gh]
***[H:\LaunchU3.exe]*** info: LastError=[126] [3872 - 5764] [31/08/2006
11:01:02.609] RunLaunchPad success
***[H:\LaunchU3.exe]*** error: LastError=[183] [3872 - 5764] [31/08/2006
11:01:02.609] CAutoPlayMgr::AddDrive h
***[H:\LaunchU3.exe]*** info: LastError=[183] [3872 - 5764] [31/08/2006
11:01:02.609] U3Launcher finished
```

FIGURE 1 Example U3Launcher.log file.

1039E4D2-DE56-4bd2-B564-7D178F5DF6F0	Weatherbug
1B285B84-A1E2-446b-ABAF-1226DAC8D60A	Electric Eddie
1ED2AA6E-626E-4159-96DD-0A8621CDEFF1	FileZilla
236C571E-47D6-4a73-AD5A-97F1E555E375	OpenOffice
573c1d30-4ba7-11da-8cd6-0800200c9a66	Irfanview
58EA136C-7E57-4416-B59E-394C46DD505B	Trillian
655F9DEA-D5ED-47aa-AE31-A6835F92A343	Party Poker
C7D3B0AA-0C02-4734-8DD3-F2C987B5D514	Winamp
DDA4889E-27C0-4DC9-91A2-F303818B211F	WinRar
EEBD498B-06AB-4e51-A706-5C4C78DA3956	FireFox

**FIGURE 2** Overview of application directories.

```
<u3manifest version="1.0">
  <application uuid="1B285B84-A1E2-446b-ABAF-1226DAC8D60A"
  version="1.1.0.0">
    <icon>icon.ico</icon>
    <name>Electric Eddie</name>
    <vendor url="http://www.300ad.com/">300AD.com</vendor>
    <description>Eddie is a passionate electrician in troubles. Help him to
    wire the
    tricky cables from batteries to bulbs in this extremely addictive puzzle
    game.
    </description>
    <options>
      <minFreeSpace>3.6</minFreeSpace>
    </options>
  </application>
  <actions>
    <appStart workingdir="%U3_DEVICE_EXEC_PATH%"
    cmd="%U3_DEVICE_EXEC_PATH%\eddie.exe"></appStart>
    <appStop cmd="%U3_HOST_EXEC_PATH%\stop.exe"></appStop>
    <hostCleanUp
    cmd="%U3_HOST_EXEC_PATH%\stop.exe">nop</hostCleanUp>
  </actions>
</u3manifest>
```

**FIGURE 3** Example Manifest.u3i file.

Besides the Manifest directory, most of the application directories also contained an Exec directory; this directory can contain the files of the application itself.

To show an example of the files in the Exec directory, the files below were found on the Exec directory of the U3 Weatherbug application.

- WxBugLiteStop.exe
- WxBugLiteGeneric.exe
- WeatherBug.exe
- AwsLiteU3Stop.adm

All the directories below the first random directory seem to have been deleted after the U3 stick was ejected, but they still were in the slack space and free space of the computer. Most of the files and directories could be found quite easily.

## Registry

The U3 stick makes a number of changes to the registry of the computer that it is being used on. Some of the registry keys that the U3 stick used in our testing environment are listed below:

- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\CdRom&Ven\_Intuix&Prod\_U3&Rev\_6.16\0D30CC50B0508885&1
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven\_Intuix&Prod\_U3&Rev\_6.16\0D30CC50B0508885&0
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#USBSTOR#CdRom&Ven\_Intuix&Prod\_U3& Rev\_6.16# 0D30CC50B0508885&1#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

- HKEY\_LOCAL\_MACHINE\SYSTEM\Current-ControlSet\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#USBSTOR#CdRom &Ven\_Intuix&Prod\_U3& Rev\_6.16# 8&22917db2 &0&0D30CC50B0508885&1#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

Once again we see the U3 stick serial number (0D30CC50B0508885) showing up. When searching on the U3 string or the serial number, quite a lot of other registry keys can be found.

The registry keys do not show much information about what has been done with the U3 stick.

## Programs on the U3 Stick

The different programs on the U3 stick leave different traces on the computer. From each program we tested we will list a couple of traces (if found) below; some of the traces were found in the slack space and free space of the computer. All the tested applications were the special U3 versions of them.

A note about the programs can be made: Some of the programs automatically started as soon as the U3 stick was inserted. To leave as little traces as possible, disabling these programs would be a good idea.

```
LAUNCHU3.EXE-25327125.pf
LAUNCHPAD.EXE-0202B3B6.pf
WXBUGLITEGENERIC.EXE-38F0C4A1.pf
MAXTHON.EXE-056598FA.pf
WEATHERBUG.EXE-1744B5DE.pf
OPENOFFICEFORU3HOSTCONFIGURE.-0BE5A270.pf
OPENOFFICEFORU3START.EXE-14D87D3F.pf
SOFFICE.EXE-05F01929.pf
SOFFICE.BIN-399B4E09.pf
LAUNCHER.EXE-18F892E3.pf
WINRAR.EXE-0C5D1AE3.pf
FIREFOX.EXE-02D99781.pf
FIREFOX.EXE-07EA0631.pf
FILEZILLA.EXE-0A63D15C.pf
I_VIEW32.EXE-0413FD0F.pf
TRILLIAN.EXE-247FD775.pf
WINAMP.EXE-1BB8BF0F.pf
ZPLAYER.EXE-0018AE5A.pf
EDDIE.EXE-25434B7B.pf
OPENOFFICEFORU3HOSTCLEANUP.EX-01081D69.pf
MEDICALERT.EXE-25A73BB5.pf
WXBUGLITESTOP.EXE-1FC450D7.pf
PARTYPOKER.EXE-21622A34.pf
PARTYGAMING.EXE-29510F05.pf
CU3CLUP.EXE-236CD998.pf
```

**FIGURE 4** List of opened executables in the prefetch directory.

## Prefetch Files

When a program from the U3 stick is opened, a prefetch file (\*.pf) will be generated in the C:\windows\prefetch directory. The files listed in this directory will contain the name of the opened executable, as shown in Figure 4.

Inside these files information can be found of the application the prefetch file is from. A couple of strings out of a prefetch file (EDDIE.EXE-25434B7B.pf) are shown in Figure 5.

The string 1B285B84-A1E2-446B-ABAF-1226DA C8D60A confirms the file name; the string is the same as we saw before (see Directories), so we know the file is for the application Electric Eddie.

## Recent Files

Right after a file from the U3 stick is opened using a U3 application, a link file (\*.lnk) will be written to the C:\Documents and Settings\\Recent directory. The link files have the same name as the opened file (except the file extension, which is changed to .lnk) and contain the following information of the opened file:

- Local path of the file
- Volume type of the disk the file is opened from
- Volume label of the disk the file is opened from

```

\DEVICE\HARDDISK1\DP(1)0-0+3\SYSTEM\APPS\
1B285B84-A1E2-446B-ABAF-1226DAC8D60A\EXEC\SDL.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SORTKEY.NLS
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\CTYPE.NLS
\DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ADMINISTRATOR\
APPLICATION DATA\U3\0D30CC50B0508885\
1B285B84-A1E2-446B-ABAF-1226DAC8D60A\EXEC\APP.PID
\DEVICE\HARDDISK1\DP(1)0-0+3\SYSTEM\APPS\
1B285B84-A1E2-446B-ABAF-1226DAC8D60A\EXEC\GAME.CFG
\DEVICE\HARDDISK1\DP(1)0-0+3\SYSTEM\APPS\
1B285B84-A1E2-446B-ABAF-1226DAC8D60A\EXEC\GAME.DAT

```

**FIGURE 5** Strings from a prefetch file showing information about the application.

- Volume serial number of the disk the file is opened from
- File size
- Creation time of the file
- Last write time of the file
- Last access time of the file

This is normal behavior for a file that is opened locally on a computer, but the U3 stick does not seem to prevent this information from being stored on the computer.

An example of the data that can be retrieved from a link file is shown below.

- Local Path E:\Documents\This file will be opened.doc
- Volume Type Removeable Disk
- Volume Label Intuix key
- Volume Serial Number 40BB-8FA5
- File size 23040
- Creation time (UTC) 3-7-2006 12:36:57
- Last write time (UTC) 3-7-2006 12:36:36
- Last access time (UTC) 2-7-2006 22:00:00

When a file from the U3 stick is opened by double-clicking it, a program to open it will be used from the computer itself and not a program from the USB stick. This will, of course, leave the same traces in the recent files directory as stated above, but it can also leave traces in the recently opened files listing of the program itself that was used to open the file.

### Program Traces

The U3 applications we tested are listed below with some more information about them and the kind of traces they left behind. If no traces are explicitly

named, the traces are found in the prefetch directory (see Prefetch Files) or the recent files directory (see Recent Files).

### Open Office

Open Office is a free and open source office suite.<sup>4</sup> While testing Open Office we mainly focused the research on the word processor.

The following actions were taken with the word processor from Open Office: Making a new document and saving it as an Open Office document; opening a Word document, editing it, saving it as a Word document, and saving it as an Open Office document.

Besides the traces that Open Office was used, there were also traces of the names of the documents we opened with Open Office.

### WeatherBug

WeatherBug is a piece of software for Microsoft Windows and Mac OS X that displays information about the weather.

Working on our investigation with dull weather outside, we checked for the weather in some sunny places. All these places could be found in the traces that were left behind on the computer. The traces could be found in the Microsoft Internet Explorer history file<sup>5</sup> and the Temporary Internet Files.<sup>6</sup>

Example Internet addresses that were found on the computer are

- [http://web.lite.weatherbug.com/World/Page/WorldObservations.aspx?zcode=Z5489&uid=c994ba2b-d7cb-4299-8705-2a62c2595246&dclid=100&world\\_stat=TNCB&city\\_id=50000&world\\_units=1&\\_KWS\\_Unit=1\\_KWE\\_&dclid=WLOU](http://web.lite.weatherbug.com/World/Page/WorldObservations.aspx?zcode=Z5489&uid=c994ba2b-d7cb-4299-8705-2a62c2595246&dclid=100&world_stat=TNCB&city_id=50000&world_units=1&_KWS_Unit=1_KWE_&dclid=WLOU)

- [http://web.lite.weatherbug.com/World/Page/WorldObservations.aspx?zcode=Z5489&uid=c994ba2b-d7cb-4299-8705-2a62c2595246&dldid=100&\\_KWS\\_Zip=\\_KWE\\_KWS\\_State=\\_KWE\\_KWS\\_CityId=50000\\_KWE\\_KWS\\_City=Flamingo\\_KWE\\_KWS\\_Country=Netherlands%20Antilles\\_KWE\\_KWS\\_StationId=TNCB\\_KWE\\_&t=62035](http://web.lite.weatherbug.com/World/Page/WorldObservations.aspx?zcode=Z5489&uid=c994ba2b-d7cb-4299-8705-2a62c2595246&dldid=100&_KWS_Zip=_KWE_KWS_State=_KWE_KWS_CityId=50000_KWE_KWS_City=Flamingo_KWE_KWS_Country=Netherlands%20Antilles_KWE_KWS_StationId=TNCB_KWE_&t=62035)

### Firefox

Firefox is a free, open source, cross-platform, graphical web browser. With Firefox the following actions were taken: Visiting a couple of web sites and performing a search query in Google. While starting the Firefox browser from the U3 stick, it went straight to the web site of YourBrainz (<http://home.yourbrainz.com>). Firefox did not seem to leave any clear traces of the actions we took with it, but it did show the fact that Firefox was used on the computer.

### Maxthon Browser

Maxthon Browser is a tabbed web browser with a customizable interface. With Maxthon we also visited a couple of web sites and we performed a search query in Yahoo!. Maxthon Browser is not as clean as FireFox is; the traces it left behind showed us the URLs we visited and the search query we performed. These traces could be found in the Microsoft Internet Explorer history file and the Temporary Internet Files.

### FileZilla

FileZilla is a free, open source FTP client for Microsoft Windows. To test FileZilla we connected to an FTP and looked around. These actions did not leave any clear traces on the computer, but there were traces of the fact that FileZilla was used.

### Trillian

Trillian is a multiprotocol instant messaging application for Microsoft Windows. While testing the U3 stick we used MSN with the Trillian application on

the U3 stick to discuss some of our findings. Afterwards we were able to find our MSN address, the address of the person we spoke to, and even fragments of the conversation we had on the computer in the page file of the computer. What was even worse is that we stumbled upon our plain text MSN password in the same page file.

The part of the page file that shows the email address and the password of our MSN account is shown in Figure 6.

### Irfanview

IrfanView is a freeware image viewer for Microsoft Windows that can view, edit, and convert image files of dozens of image formats and play over a dozen video/audio formats. With Irfanview we viewed a couple of pictures and also edited some of them. We found the file names of the pictures we viewed, but we did not find the pictures themselves on the computer.

### WinAmp

WinAmp is a multimedia player. We used WinAmp to listen to some songs in the MP3 format; afterwards we were able to find the names of all the songs we listened to. We were not able to find the songs themselves on the computer. The names of the songs we listened to could be found in the Microsoft Internet Explorer history file.

### Party Poker

Party Poker is a big online poker room program. We tested Party Poker by starting it without actually playing poker online. When starting Party Poker it started Microsoft Internet Explorer and downloaded and installed an update. These actions, of course, left a lot of traces behind in the Microsoft Internet Explorer history file as well the Temporary Internet Files on the computer.

The update was downloaded to the computer and then the files were written to the U3 stick. The files that have been downloaded could be found in the

```

orization: Passport1.4
OrgVerb=GET,OrgURL=http%3A%2F%2Fmessenger%2Emsn%2Ecom,sign-
in=testmsn%40
fox-
it%2Ecom,pwd=FoxFoxFox,lc=1033,id=507,tw=40,fs=1,ru=http%3A%2F%2Fmesse
nger
%2Emsn%2Ecom,ct=1151933376,kpp=1,kv=7,ver=2.1.6000.1,rn=5BN3aTLN,tpf=a
a8573130ff111d382b1e2efdcf6b8ca

```

**FIGURE 6** Part of page file containing a MSN account and password.

```
e:\system\apps\655f9dea-d5ed-47aa-ae31-a6835f92a343\exec\stealth\partypoker\
tmpUpgrade\..\PartyGaming.exe
e:\system\apps\655f9dea-d5ed-47aa-ae31-a6835f92a343\exec\stealth\partypoker\
PartyPoker\tmpUpgrade\..\PartyCasino\GRA.ini
e:\system\apps\655f9dea-d5ed-47aa-ae31-a6835f92a343\exec\stealth\partypoker\
PartyPoker\tmpUpgrade\..\PartyCasino\Images\active_popup-right.JPG
e:\system\apps\655f9dea-d5ed-47aa-ae31-a6835f92a343\exec\stealth\partypoker\
PartyPoker\tmpUpgrade\..\PartyCasino\Images\active_title-topleft.JPG
e:\system\apps\655f9dea-d5ed-47aa-ae31-a6835f92a343\exec\stealth\partypoker\
PartyPoker\tmpUpgrade\..\PartyCasino\Images\active_title-
background.JPG
e:\system\apps\655f9dea-d5ed-47aa-ae31-a6835f92a343\exec\stealth\partypoker\
PartyPoker\tmpUpgrade\..\PartyCasino\Images\active_title-topleft.gif
```

**FIGURE 7** Party Poker update files named in the registry.

registry in the key HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls

A couple of the files that are named in the registry are listed in Figure 7.

### *MedicAlert*

MedicAlert is a tool that can be used to record your personal medical information. To test MedicAlert we used it where it should be used to record some of our personal medical information. MedicAlert did not seem to leave any of our personal medical records lying around and so no traces of them were found.

### *Winrar*

WinRAR is a shareware file archiver and data compression utility. WinRAR can be used to archive and unpack files, and that is what we did with it. We unpacked a Zip-archived file and we added a document to a new archive. The name of the Zip-archived file could be found on the computer; the name of the document we added to the archive as well as the archive itself could not be found.

### *Electric Eddie*

Electric Eddie is a game in which you play “a passionate electrician in troubles.” To relax a little from all the testing we played a little game with Electric Eddie, our electrician. Because we should not have been playing games at work instead of working, we hoped Eddie would not leave any traces of the game behind. But Eddie did, and the traces on the computer showed that we had been playing the game.

These findings show us that all the applications that have been used from the U3 stick left traces behind that show the use of the applications. Some of the applications went a little further and also revealed

information about the actions that were taken and the file names of the files that were opened.

## CONCLUSION

While being a neat and useful gadget, the U3 stick does not completely do what it states to do. The stick can indeed be used to take your favorite programs and files with you and use them on any computer you like (if the computer allows this, of course). But the U3 stick and most of the programs on it (at least the ones we tested) do leave traces on the computer it has been used on, which is something to keep in mind before using the U3 stick—and, of course, also something to keep in mind when examining a computer the U3 stick has been used on.

Most of the traces the U3 stick leaves behind can be found in the slack space and the free space of the computer it has been used on. These traces are not clear for every computer user, but those kinds of traces should not be a problem at all for a forensic IT investigator.

To conclude, at this moment the U3 stick gives a forensic IT investigator enough traces to find out it that has been used and it leaves quite a few traces that give an idea what has been done with it.

## NOTES

1. Translated from Dutch.
2. Translated from Dutch.
3. Assuming that the Microsoft Windows operation system is installed on the C: disk drive.
4. Descriptions are taken from Wikipedia (<http://en.wikipedia.org>) or the vendor's web site where available.
5. Documents and Settings\\LocalSettings\History\History.IE5\index.dat
6. Documents and Settings\\LocalSettings\Temporary Internet Files\Content.IE5\index.dat

## REFERENCES

1. U3 website (2006). U3 Benefits. U3 website. Retrieved December 5, 2006, from <http://www.u3.com/platform/benefits.aspx>
2. Dennis, T. (2005). U3 promises totally mobile apps. The Inquirer. Retrieved December 5, 2006, from <http://www.theinquirer.net/?article=20588>
3. PCWorld (2005). USB Drives Get Two Thumbs Up. PCWorld Website. Retrieved December 5, 2006, from <http://www.pcworld.com/digitalduo/article/0,aid,123973,00.asp>
4. Kerstholt, W. (2005). U3 USB-standard voor gesteld door Sandisk en M-systems. Tweakers net website. Retrieved December 5, 2006, from <http://www.tweakers.net/nieuws/35660>
5. Computer Idee (2006). Slimme staaf: Intuix SmartDrive S30D. Computer idee 02–2006 (09/01–23/01)

