their respective countries. Furthermore, there are cases where investigators (especially security officers) are requested to manage international sexual harassment cases that involve several types of digital evidence. This happens especially within multinational corporations. Despite the fact that corporate policies are released by the headquarters, please be aware that such policies may be not applicable in a particular branch located in another jurisdiction because they are not compliant with local regulations.

Going to court: testifying or justifying

We would point out to the importance of proper court testimony. Whether you are a 'simple' or 'expert' witness, you will be required to maintain behaviour based on integrity and ethics. Such ethics can be regulated by law and/or codes. An example of a code of ethics for digital investigators is provided by IACIS[1]. A similar one for 'conventional' PI is offered by the Association of British Investators[2]. If you compare those two examples, you will find many similarities that provide further examples of convergence in the two fields.

At the current moment in history, we have a number of examples of how a bad witness (or non-compliant evidence handling) could have a negative impact on the court case. We cannot exclude the possibility of it generating a sort of multi-level legal liability. So it is clear that there is no difference between private investigators, digital investigators or similar operators in the event of error.

References

1. Code of Ethics, International Association of Computer Investigative Specialists, Accessed January 2009 <http://www.iacis.com/new_membership/code_of_ethics>
2. Code of Ethics, Association of British Investigators, Accessed January 2009 <http://www.theabi.org.uk/about/ethics.htm>

About the author

Dario Forte, CFE, CISM, former police detective and founder of DFLabs, has worked in information security since 1992. He has been involved in numerous international conferences on information warfare, including the RSA Conference, Digital Forensic Research Workshops, the Computer Security Institute, the US Department of Defense Cybercrime Conference, and the US Department of Homeland Security (New York Electronic Crimes Task Force). He was also the keynote speaker at the Black Hat conference in Las Vegas. He provides security consulting, incident response and forensics services to several government agencies and private companies.
www.dflabs.com

Fighting forensics

Steve Mansfield-Devine

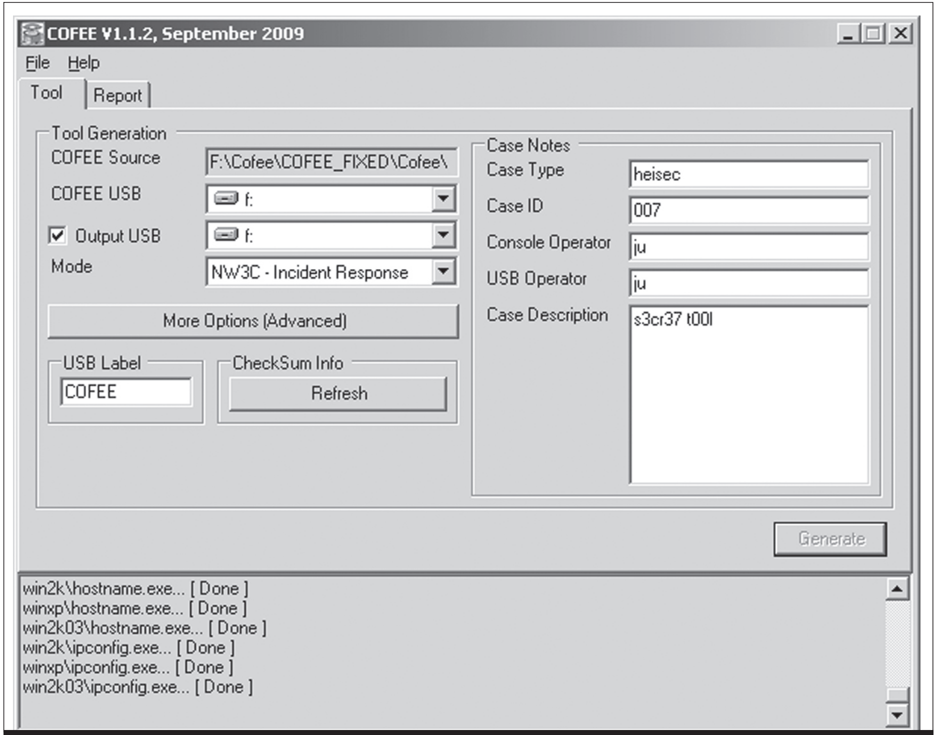
Steve Mansfield-Devine

Since crime began, the bad guys have tried to cover their tracks. For every advance in forensics and criminal detection, there has been a countermeasure. When fingerprinting was invented, burglars started wearing gloves. When hackers gain root on a remote system, they take care to delete log files to mask what they've done. And as IT forensics methods have improved, so have the anti-forensics techniques designed to defeat them.

COFEE spilled

The issue of anti-forensics gained a higher profile recently with the leak of a forensics tool from Microsoft. Dubbed COFEE (Computer Online Forensic Evidence Extractor), it's actually a bundle of readily available tools designed to be used by police officers on Windows PCs found at the scene of a crime. In theory, by running within a shell from a USB flash drive, COFEE gathers system information without compromising any later, more in-depth forensic investigation. It's intended to be used by inexperienced officers purely for information gathering.

An autorun script invokes a number of command-line tools — as many as 150 commands. Most of these will be familiar to sysadmins as they are available from SysInternals, MS Resource Kits and from the internet. For capturing volatile data, for example, COFEE invokes ipconfig, nbtstat, net, pslist, whoami, quser, psloggedon, netstat, sclist, showgrps and systeminfo, among others. Its 'incident response' mode calls tools such as at, autoruns, getmac, handle, hostname, ipconfig, msinfo32, nbtstat, net, netdom, netstat, openfiles, pslist, psloggedon,



Tool Generation
COFEE Source: F:\Cofee\COFEE_FIXED\Cofee\
COFEE USB: f:
☑ Output USB: f:
Mode: NW3C - Incident Response

Case Notes
Case Type: heisec
Case ID: 007
Console Operator: ju
USB Operator: ju
Case Description: s3cr37 t00l

USB Label: COFEE
CheckSum Info

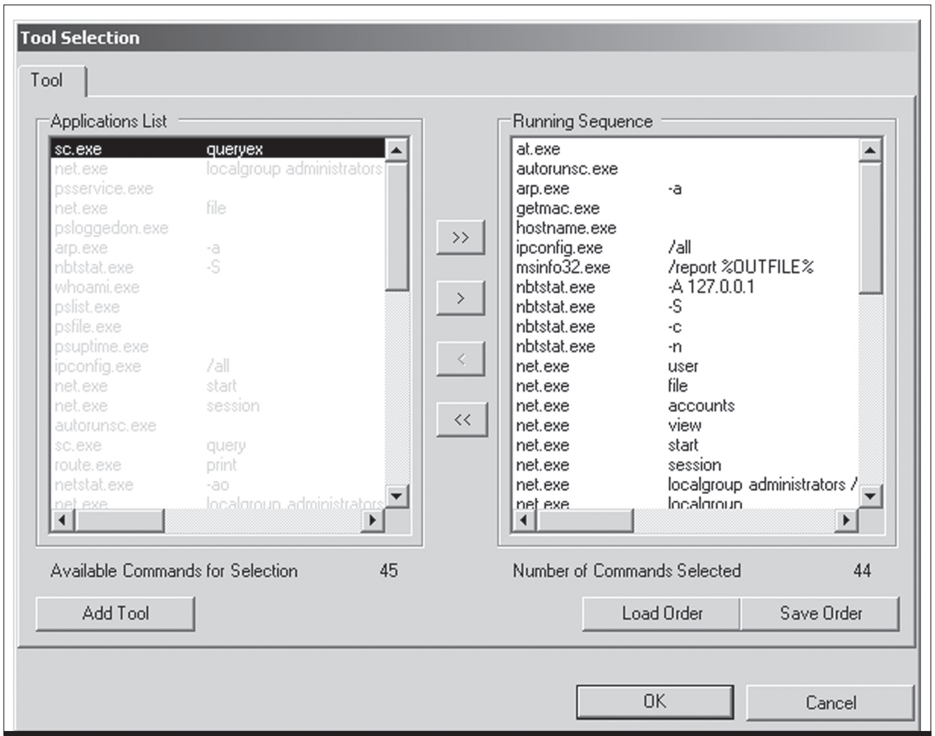
```
win2k\hostname.exe... [ Done ]
winxp\hostname.exe... [ Done ]
win2k03\hostname.exe... [ Done ]
win2k\ipconfig.exe... [ Done ]
winxp\ipconfig.exe... [ Done ]
win2k03\ipconfig.exe... [ Done ]
```

Figure 1: COFEE is first installed on a PC where it is then loaded on to a USB flash drive. This screen shows the flash drive install set-up.

psservice, pstat, psuptime, quser, route, sc, sclist showgrps, srvcheck, tasklist and whoami. All the commands come with preset options.

But not everyone is allowed to have COFEE. Microsoft makes it available only to qualified law enforcement organisations. In the US it's supplied by the National White Collar Crime Center (NW3C), and worldwide it's distributed by Interpol.

That all went pear-shaped when Cryptome.org made it available for download from its website. Inevitably, copies became available via BitTorrent and warez sites. It's still easy to find.



Applications List

```
sc.exe          queryex
net.exe         localgroup administrators
psservice.exe
net.exe         file
psloggedon.exe
arp.exe         -a
nbtstat.exe     -S
whoami.exe
pslist.exe
psfile.exe
psuptime.exe
ipconfig.exe    /all
net.exe         start
net.exe         session
autorunsc.exe
sc.exe          query
route.exe       print
netstat.exe     -ao
net.exe         localgroup administrators
```

Available Commands for Selection 45

Running Sequence

```
at.exe
autorunsc.exe
arp.exe         -a
getmac.exe
hostname.exe
ipconfig.exe    /all
msinfo32.exe    /report %OUTFILE%
nbtstat.exe     -A 127.0.0.1
nbtstat.exe     -S
nbtstat.exe     -c
nbtstat.exe     -n
net.exe         user
net.exe         file
net.exe         accounts
net.exe         view
net.exe         start
net.exe         session
net.exe         localgroup administrators /
net.exe         localgroup
```

Number of Commands Selected 44

Figure 2: Users of COFEE can choose which tools to run and in which order.

Playing it down

Microsoft's response to the leak was, perhaps predictably, to play it down. The company issued a statement that said, in part:

"In theory, by running within a shell from a USB flash drive, COFEE gathers system information without compromising any later, more in-depth forensic investigation"

"We do not anticipate the possible availability of COFEE for cybercriminals to download and find ways to 'build around' to be a significant concern. COFEE … is essentially a collection of digital forensic tools already commonly used … Its value for law enforcement is not in secret functionality unknown to cybercriminals; its value is in the way COFEE brings those tools together in a simple and customisable format".

Presumably, however, the data collected by COFEE is important — otherwise, why bother? If it can be prevented from working, an investigation might be left with no IT forensics evidence. Understanding how COFEE works — which tools it deploys and how those are invoked — is useful information to any wanting to defeat it. And so it proved. Once again, Microsoft's approach of security through obscurity failed.

Enter DECAF

The countermeasure to COFEE is called DECAF (Detect and Eliminate Computer-Assisted Forensics).[1] If a machine running DECAF detects a USB drive with COFEE, it attempts to lock down the computer and start covering tracks. It performs the following actions:

- Contaminate or spoof MAC addresses
- Kill running processes
- Disable network adapters, USB ports, floppy drive, CD-ROM and serial and printer ports
- Erase data including directories (as per user configuration)

- Clear the Event Viewer and remove its logs
- Remove torrent clients, including Azureus and BitTorrent
- Remove cookies, browser cache and history
- Power down the PC

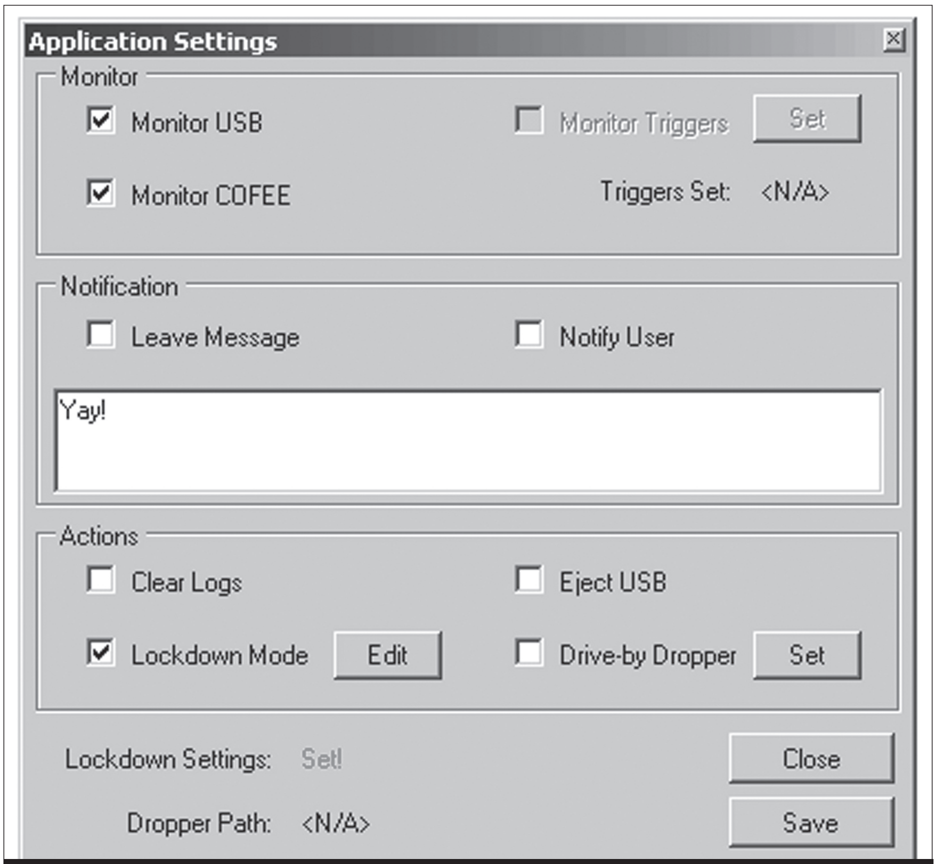
The people who produced the tool claimed they "weren't out to obstruct the collection of evidence". Like many hackers, they claimed the purpose was to encourage the production of better forensic tools — which is a little like calling burglary a plea for better alarms.

In fact, when told that the software might attract legal problems, version 1 of DECAF was withdrawn and the software authors claimed it was all a stunt. They 'deactivated' DECAF: the tool called home via HTTP when run, and if it didn't get the right response, it crashed. But at least one blogger demonstrated how to get around that.[2]

They seem to have got over their legal worries, having now produced version 2. As well as watching out for COFEE, this is also on the alert for Helix, EnCase, Passware, Elcomsoft, FTK Imager Port, Forensic Toolkit, ISOBuster and ophcrack. And users can add their own signatures.

The fuss about the original leaking of COFEE and the appearance of DECAF is all a bit of a storm in a … well, coffee cup perhaps. Some forensics experts doubt the evidential value of data collected by COFEE. It is aimed at 'first responders', but there's a strong argument that such people, with no IT forensics training, shouldn't be going anywhere near suspect PCs.

Besides, who would actually use DECAF? And would the presence of DECAF on a machine itself be incriminating?



Application Settings

Monitor

☑ Monitor USB

□ Monitor Triggers

☑ Monitor COFEE

Triggers Set: <N/A>

Notification

□ Leave Message

□ Notify User

Yay!

Actions

□ Clear Logs

□ Eject USB

☑ Lockdown Mode

□ Drive-by Dropper

Lockdown Settings: Set!

Dropper Path: <N/A>

Figure 3: DECAF offers a number of options, including a configurable 'lock down' mode that deletes files and even whole directories.

Classic tools

DECAF is just the latest in a long line of techniques used by people who don't want their activities to show up in a forensic analysis. Most are geared towards defeating direct investigation of PCs. Encryption is a common method: TrueCrypt, for example, boasts that it provides plausible deniability by not only encrypting a file but disguising or hiding it too. There are other methods of hiding data, such as using sections of a disk marked by the OS as system space, bad blocks or unallocated (tools for this include Slacker, FragFS, RuneFS and others) or steganography. Then there are tools such as Timestomp which messes with file creation, modification and access data, rendering them useless as evidence.

What makes DECAF interesting is that it is a system designed to operate automatically by detecting when a system is being analysed. And it is not alone in doing that. We've seen anti-forensic software designed to attack investigators by, for example, exploiting buffer overflows in certain versions of the tools that investigators use, such as tcpdump, Snort and Ethereal. Anti-forensic software might also watch for the signs that analysis tools may be in use — such as hosts being in promiscuous mode and responding unusually to pings, ARPs and malformed packets. One anti-forensic measure is to transmit a packet with a fake IP address and watch for a reverse-DNS lookup.

Botnet reprisals

Botnets have been known to have built-in defence mechanisms, usually resulting in distributed denial of service (DDoS) attacks being launched against the IP address of anyone trying to infiltrate them.

"It happened to me with Storm," says David Sancho, an anti-malware researcher with TrendLabs. "It's difficult to know how this was implemented because it was a back-end process. But suddenly you were flooded with packets coming from everywhere." On another occasion, TrendLabs' automated analysis tools encountered the website used as a lure by Storm. The HTML code contained a link that was commented out, but the automated tools didn't know that. The Trendlabs machine followed the link and provoked a DDoS attack as a result.

These kinds of mechanisms are not that common on botnets any more, Sancho says. They have other means of protection now. These days, the place you're most likely to encounter automated anti-forensics is in malware.

Malware protection

Chad Loeven, VP and general manager of Sunbelt Software's SunbeltLabs, estimates that around a third or more of malware has anti-forensics built in, and the proportion is increasing all the time.

"One factor is the propagation of malware SDKs, plus code freely available in forums," he says. "There's sample code on the internet that you just copy and paste right into your malware that will do fairly sophisticated checking for specific analysis tools. The malware not only knows that it's being analysed, it knows what is trying to analyse it."

Malware writers have implemented a whole bag of tricks to get around anti-virus (AV) software on an infected machine. Viruses attempt to uninstall AV software (sometimes by invoking its own uninstall package), corrupt or replace the malware database or change update version numbers.

"It can be as simple as creating entries in the HOSTS file so that, say, trendmicro.com points to 127.0.0.1," says Sancho. "That's an old one but still very effective."

In one notorious case, a piece of malware replaced Kaspersky software with a hacked version, designed to detect all viruses except itself.

Anti-analysis

Malware writers also specifically target the forensics efforts of researchers. "One crude method is that they'll actually track the IP blocks of the main security researchers," says Loeven. Malware will call home and check its current IP against a list, or have a built-in block list. If a known IP is encountered, the malware switches off.

An old, notorious and yet effective technique, still in widespread use, is to check if the operating system is being run in a VMware environment. Anti-malware researchers often use VM because the virtual machines provide a robust form of sandboxing, and it allows them to run large numbers of environments very cost-effectively. If the malware detects a VM environment, it simply does nothing, so that the analysis tools don't detect it. "The malware SDKs out there even have a switch in the compiler that says 'check this box if you want to have anti-VM capability'," says Loeven. Sunbelt, he says, has abandoned VM and carries out its analysis on machines running Windows natively.

Sophistication/ effectiveness

That doesn't mean that anti-forensics are necessarily effective. "Clearly, some of the techniques they use rely on oversights on the part of the people doing the analysis, or they try to take advantage of stuff that was patched a long time ago," says Loeven. In addition, AV companies have access to the same SDKs and code the malware writers are using, and can take steps accordingly — the reverse situation of COFEE/DECAF.

"Nevertheless, there are some very clever guys out there," says Loeven. "We had one piece of malware that, as it was executing inside our analysis systems, was taking screenshots and sending them back to a command and control server. The malware authors were getting screenshots of our analysis tools running, with directories and everything."

Sancho agrees that the level of sophistication is increasing rapidly. The motive is money, he says: the bad guys are organised criminals with big budgets to hire the best skills. "If you come up with a new form of protection or detection," he says, "they'll spend two, three months until they break it."

References

1. DECAF web page, http://decafme.org
2. Praetorian Prefect blog: http://praetorianprefect.com/archives/2009/12/reactivating-decaf-in-two-minutes/

Calendar

15 – 18 February
WSDF 2010
Location: Krakow, Poland
Website: http://www.ares-conference.eu/conf/index.php/workshops/wsdf

1 – 5 March
RSA 2010
Location: San Francisco, CA, USA
Website: http://www.rsaconference.com

14 – 17 March
GRC Summit 2010
Location: Amelia Island, FL, USA
Website: http://www.grcsummit2010.com/Home_Page.htm

19 – 20 March
CarolinaCon
Location: Raleigh, NC, USA
Website: http://www.carolinacon.org/

23 – 24 March
Boston SecureWorld Expo 2010
Location: Boston, MA, USA
Website: ttp://www.net-security.org/conference.php?id=367

23 – 25 March
ISC West
Location: Las Vegas, NV, USA
Website: http://www.iscwest.com/

25 – 26 March
MIT Spam Conference
Location: Cambridge, MA, USA
Website: ttp://projects.csail.mit.edu/spamconf/#top

27 – 28 March
ARSPA -WITS '10
Location: Paphos, Cyprus
Website: ttp://www.avantssar.eu/arspa-wits10/