Digital Village | Hal Berghel

The Discipline of Internet Forensics

A well-defined field of study and practice has evolved as a result of network hacker activity.

In a past *Communications* column in ("The Profession of IT," Feb. 2001), Peter Denning identified the four hallmarks of a profession: a durable domain of human concerns; a codified body of principles (conceptual knowledge); a codified body of practices (embodied knowledge including competence); and standards for competence, ethics, and practice. Denning added that professions also include institutions for preserving the knowledge and practice, enforcing the standards, and educating professionals.

Although Denning's discussion related to IT as a whole, I want to drill down a bit into a subdiscipline that deserves more recognition and separate status than it is currently receiving: network or Internet forensics (hereafter just Internet Forensics). At this point, Internet Forensics has not been fully appreciated because of its proximity, historically and conceptually, with computer forensics—which I would argue is actually more different than similar from its networking cousin. As a result, the two tend to be evolving together, when they should be evolving separately.

Meeting the Four Criteria

Denning argued that IT clearly satisfies the first two conditions, partially satisfies the last two, and is likely to satisfy all four within the next decade. He was also careful to distinguish disciplines and professions from crafts and trades, and to distinguish his broader interpretation of a profession from the narrower definition of a profession as a "set of people who have at least two years of post baccalaureate education and whose field is on an approved list" proffered by the U.S. Department of Education.

While not a profession, computer forensics satisfies the definition of a discipline. It is a well-defined field of study and practice. Like IT itself, it satisfies both the durability condition and the body of principles. It also has a codified body of practices that have evolved over the years through courtroom experience, and standards for competence, ethics, and practice.

The SANS Institute (www.sans.org), for example, offers courses in computer security, and the Global Information Assurance Certification (www.giac.org) offers a certificate in Certified Forensic Analysis that requires renewal every four years and has a Code of Ethics (www.giac.org/COE.php) with which each certificate holder must agree. Standard textbooks exist, as do articles. Conferences, such as the Digital Forensics Research Workshop (www.

ROBERT NEUBECKER

Computer Forensics was championed early on by law enforcement and fits well within its overall investigative methodology. Internet Forensics, on the other hand, evolved as a response to the hacker community. In fact, Internet Forensics specialists have essentially the same skill sets as their adversaries.

dfrws.org), have been held and peer-reviewed journals like the *International Journal of Digital Evidence* (www.ijde.org) have been developed, just as one might expect of a rapidly maturing discipline.

Much the same may be said of network or Internet Forensics, but the subject area occupies a far less independent role in the computing security community. In one of life's ironies, it was Internet security concerns that actually helped drive Computer Forensics to the disciplinary status it now enjoys.

Computing vs. Internet Forensics

There is no question that computer forensics is more familiar to the IT community. My Google search produced 60,600 hits for "computer forensics," 3,250 for "network forensics," and 146 for "Internet Forensics." However, if one looks to the skilled practitioner community, one gets a very different view. As one datapoint, consider the following list of SANS course offerings (from the SANS training matrix on www.sans.org):

Track 1: SANS Security Essentials and the CISSP CBK.
Track 2: Firewalls, Perimeter Protection, and VPNs.
Track 3: Intrusion Detection In-Depth.
Track 4: Hacker Techniques, Exploits, and Incident Handling.
Track 5: Securing Windows.
Track 6: Securing Unix.
Track 7: Auditing Networks, Perimeters, and Systems.
Track 8: System Forensics, Investigations, and Response.
Track 9: SANS Information Security Officer Training.
Track 10: IT Security Audit Essentials.
Track 12: SANS Security Leadership Essentials for Managers.

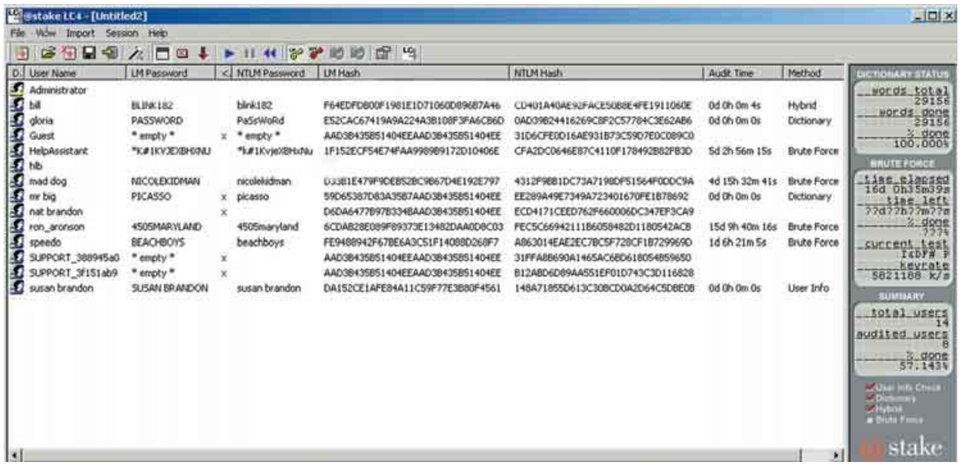
If we eliminate the basic, vanilla tracks (1 and 12), we see that of the remaining 10 tracks, only one (Track 8) focuses on computing forensics—90% are oriented primarily toward topics within network security, the detection and analysis aspect of which is Internet Forensics. So how is it that Internet Forensics is so little known outside the community that practices it?

The answer lies in the source of the inspiration of these two areas. Computer Forensics was championed early on by law enforcement and fits well within its overall investigative methodology. Internet Forensics, on the other hand, evolved as a response to the hacker community. In fact, Internet Forensics specialists have essentially the same skill sets as their adversaries. This is not the case in Computer Forensics.

The Origin of "Forensics"

The art of forensics derived from the practice of forensic medicine, which was already recognized as a medical specialty by the end of the 18th century. The most common forensic activity in this area is the autopsy, or postmortem examination, based on a general knowledge of the anatomy inherited from Pharaonic Egypt and ancient Greece (although the association between the state of the anatomy and the cause of death remained the subject of wild speculation until well into the last few hundred years).

As forensic medicine evolved from the study of anatomy, criminal forensics evolved from the study of fingerprints. So far as I can determine, no proof exists that it is impossible for more than one person to have the same fingerprints. According to Gordon Dechman, President of Fingerprint USA (www.fpusa.com), "Fingerprint patterns are genetically established, but the actual ridge structure is developed through a chaotic process, and the probability of identical fingerprints is very, very small. Fingerprints are accepted by all courts worldwide as positive proof of identity, and a considerable body of knowledge has been established and is legally accepted regarding fingerprint identification methods." The British standard, for example, holds that if two fingerprints share 16 characteristics, they are from the same individual.



D.	User Name	LM Password	<	NTLM Password	LM Hash	NTLM Hash	Audit Time	Method
	Administrator							
	bill	BLINK182		blink182	F64EDFD800F1981E1D71060D89687A46	CD401A40AE92FACE5088E4FE1911060E	0d 0h 0m 4s	Hybrid
	gloria	PASSWORD		PaSsWoRd	E52CAC67419A9A224A3B108F3FA6CB6D	0AD39B24416269C8F2C57784C3E62AB6	0d 0h 0m 0s	Dictionary
	Guest	* empty *	x	* empty *	AAD3B435B51404EEAAD3B435B51404EE	31D6CFE0D16AE931B73C59D7E0C089C0		
	HelpAssistant	*K#1KVJEXBHXNU		*k#1KvjeXBHxNu	1F152ECF54E74FAA9989B9172D10406E	CFA2DC0646E87C4110F178492B82FB3D	5d 2h 56m 15s	Brute Force
	hlb							
	mad dog	NICOLEKIDMAN		nicolekidman	D33B1E479F9DEB52BC9B67D4E192E797	4312F9BB1DC73A7198DF51564F0DDC9A	4d 15h 32m 41s	Brute Force
	mr big	PICASSO	x	picasso	59D65387D83A35B7AAD3B435B51404EE	EE289A49E7349A723401670FE1B78692	0d 0h 0m 0s	Dictionary
	nat brandon		x		D6DA6477B97B334BAAD3B435B51404EE	ECD4171CEED762F660006DC347EF3CA9		
	ron_aronson	4505MARYLAND		4505maryland	6CDAB28E089F89373E13482DAA0D8C03	FEC5C66942111B6058482D1180542ACB	15d 9h 40m 16s	Brute Force
	speedo	BEACHBOYS		beachboys	FE9488942F67BE6A3C51F14088D268F7	A863014EAE2EC7BC5F728CF1B729969D	1d 6h 21m 5s	Brute Force
	SUPPORT_388945a0	* empty *	x		AAD3B435B51404EEAAD3B435B51404EE	31FFA8B690A1465AC6BD618054B59650		
	SUPPORT_3f151ab9	* empty *	x		AAD3B435B51404EEAAD3B435B51404EE	B12ABD6D89AA551EF01D743C3D116828		
	susan brandon	SUSAN BRANDON		susan brandon	DA152CE1AFE84A11C59F77E3B80F4561	148A71855D613C308CD0A2D64C5D8E08	0d 0h 0m 0s	User Info

DICTIONARY STATUS
words total
29156
words done
29156
% done
100.000%

BRUTE FORCE
time elapsed
16d 0h35m39s
time left
??d??h??m??s
% done
???%
current test
I&DF# P
keyrate
5821188 k/s

SUMMARY
total users
14
audited users
8
% done
57.143%

☑ User Info Check
☑ Dictionary
☑ Hybrid
■ Brute Force

Figure 1. Password cracking on Windows XP with the latest commercial version of Lophtcrack, LC4 (atstake.com).*

Fingerprints have been routinely taken, categorized, and filed for over 100 years, and since the 1980s have been digitized, stored, shared, and compared on networked computer systems. This evolutionary path to computation came at a time when computers moved beyond calculation to media processing, so law enforcement investigators and prosecutors were driven to increase the level of technology in their skill sets.

So the concept of "forensics" is anything but new. However, its use in the IT arena began in the last few decades as "computer forensics."

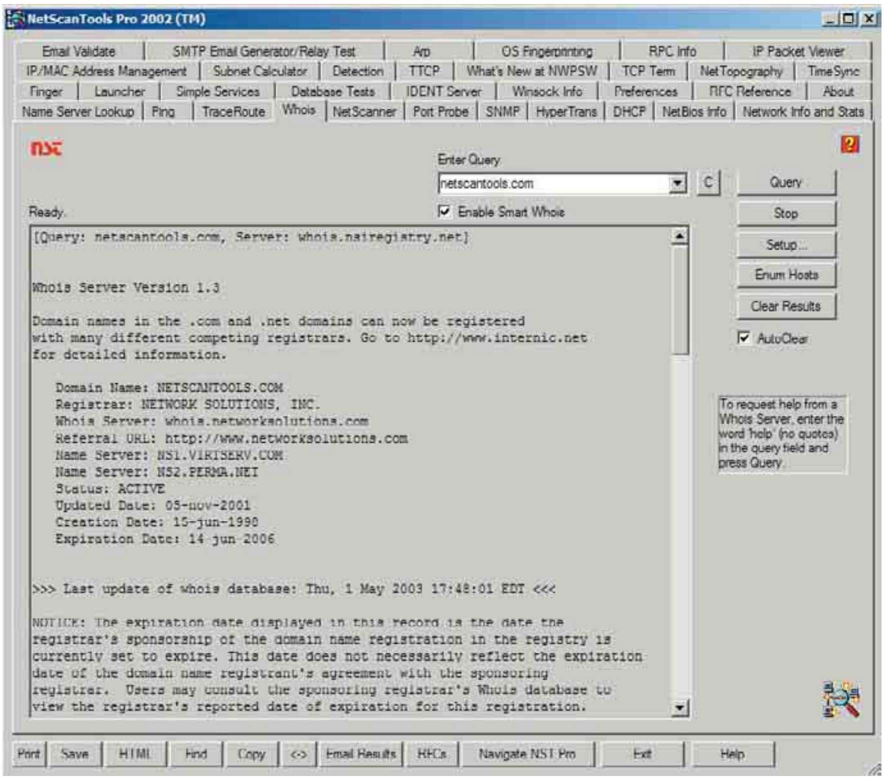
Computer Forensics

As mentioned earlier, the widespread use of computer forensics resulted from the convergence of two factors: the increasing dependence of law enforcement on computing (as in the area of fingerprints) and the ubiquity of computers that followed from the microcomputer revolution. As computer forensics evolved over time, it was modeled after the basic investigative methodologies of law enforcement and the security industry that championed its use.

Not surprisingly, computer forensics is about the "preservation, identification, extraction, documentation, and interpretation of computer data" (see the book by Kruse and Heiser listed in the Further Reading section at the end of this column). In order to accomplish these goals, there are well-defined procedures, also derived from law enforcement, for acquiring and analyzing the evidence without damaging it, while also authenticating it and providing a chain-of-custody that will hold up in court.

The tools for the "search-and-seizure" side of computer forensics are a sophisticated potpourri primarily focused on the physical side of computing: tracing and locating computer hardware, recovering hidden data from storage media, identifying and recovering hidden data (for example, watermarks—see my November 1997 column, "Watermarking Cyberspace"), decrypting files, decompressing data, cracking passwords (see Figure 1), "crow-

*Some noteworthy observations: (1) HelpAssistant, and "Support" accounts, and passwords ship with XP—there's no way to get rid of these accounts—hmmmm. (2) LC4 does the "cracking" on the old Lan Manager (LM) hash technology inherited from OS/2, which is relatively easy to break. NTLM passwords involve a relatively robust password-hashing algorithm, but that advantage is removed by default because XP automatically converts NTLM to the easily breakable LM hash for backward compatibility. Given enough time, LC4 will break every LM hash, so the "fix" is to disable the LM hash capability in the registry and sacrifice the backward compatibility. (3) We ran LC4 on this workstation for slightly more than 16 days (57% of a complete run), and recovered all but three passwords. (4) Three of the passwords were cracked in under one second. (5) LC4 can be deployed over a network.



Enter Query: netscantools.com

☑ Enable Smart Whois

Ready.

```
[Query: netscantools.com, Server: whois.nsiregistry.net]


Whois Server Version 1.3

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: NETSCANTOOLS.COM
   Registrar: NETWORK SOLUTIONS, INC.
   Whois Server: whois.networksolutions.com
   Referral URL: http://www.networksolutions.com
   Name Server: NS1.VIRTSERV.COM
   Name Server: NS2.PERMA.NET
   Status: ACTIVE
   Updated Date: 05-nov-2001
   Creation Date: 15-jun-1998
   Expiration Date: 14-jun-2006


>>> Last update of whois database: Thu, 1 May 2003 17:48:01 EDT <<<

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

To request help from a Whois Server, enter the word 'help' (no quotes) in the query field and press Query.

Figure 2. One of the more full-featured network tools, NetScanTools Pro (www.netscantools.com). Note the abundance of features built into one product.

barring” an operating system (bypassing normal security controls and permissions), and so forth. Readers old enough to remember the original Norton Utilities for DOS might consider these modern tools as the original Norton Disk Editor for DOS on steroids.

Following are some common categories and a few examples of computer forensics toolkits:

- File Viewers: Quick View Plus (ww.jasc.com)
- Image Viewers: ThumbsPlus (www.cerious.com)
- Password Crackers: l0phtcrack or LC4 (atstake.com)
- Format-Independent Text Search: dtsearch (www.dtsearch.com)
- Drive Imaging: Norton Utilities’ Ghost (www.symantec.com)
- Complete Computer Forensics Toolkits: Forensics Toolkit (www.foundstone.com); Coroner’s Toolkit (www.fish.com/tct); ForensiX (www.all.net); Computer Incident Response Suite (forensics-intl.com/tools.html); and EnCase Forensic (www.encase.com)
- Forensic Computer Systems: Forensic-Computers (www.forensic-computers.com)

Most computer forensics vendors offer a variety of tools, some even offer complete suites. But the preceding links provide a useful, high-level overview of the world of computer forensics and the tools used therein. A cursory review of this list suggests tools that are not mainstream for the typical computer villain.

Internet Forensics

I indicated earlier that the impetus for computer forensics came from law enforcement—a community that arrests, investigates, seizes, locks up, and stores physical objects. The computer forensics specialist’s adversary, in all likelihood, is a computer-using criminal with no particular skill level beyond that of a typical end user. Such is not the case with Internet Forensics.

A cursory review of the preceding list of computer forensics tools suggests they are not in widespread use by the typical computer villain. The pornographer might use a graphics tool to morph the images into something unrecognizable immediately, but that’s unlikely to be anywhere near as challenging as doing a reverse-morph on an unknown file format. The computer forensics specialist works on a different plane from the person being investigated. To the contrary, the Internet Forensics specialist uses many of the same tools and engages in the same set of practices as the person being investigated. I will illustrate with a few examples referencing Figure 2.

Suppose you've received some suspicious email and want to verify the authenticity of a URL included within. A number of options are available. One might use a browser to access information from the American Registry for Internet Numbers (www.arin.net). Or one might use any number of OS utilities. But we'll save ourselves some time and worry and use a general network appliance, NetScanTools Pro (see Figure 2). We see from the figure that in this case we identified the registration, domain name servers, and currency information for netscantools.com.

Now let's change the scenario slightly. Suppose we had some hostile intent and wanted to ferret out information about some company's network infrastructure. What tool might we use? You guessed it, NetScanTools Pro. The point is that the self-same tool is equally useful to the hacker conducting basic network reconnaissance and the legitimate Internet security specialist who's trying to determine whether a URL links to a legitimate company or a packet "booby trap." The point is that both of these uses require essentially the same skill sets.

I am not suggesting that NetScanTools Pro is a hacker tool. It is a general-purpose network analyzer. I use it all the time to analyze my networks and explain network analysis issues to my students. But in order to serve in that capacity, it must also have the capabilities to be misused by hackers. In Internet Forensics it is customarily the case that the forensics specialist undergoes the same level of education and training as the hacker he or she seeks to thwart. The difference is one of ethics, not skill. We observed that this was not true of the perpetrator and investigator in computer forensics.

To emphasize the point, look at the other options that NetScanTools Pro provides. One can use an ICMP "ping" to identify whether a particular network host is online as easily as one can use it to identify activity periods in network reconnaissance or a network topology. One can use a Traceroute to determine network bottlenecks or identify intervening routers and gateways for possible man-in-the-middle attacks. One can use Port Probe to verify that a firewall is appropriately configured or to make a list of vulnerable services on a host that may be exploited.

Where computer forensics deals with physical things, Internet Forensics deals with the ephemeral. The computer forensics specialist at least has something to seize and investigate. The Internet Forensics specialist only has something to investigate if the packet filters, firewalls, and intrusion detection systems were set up to anticipate the breach of security. But, if one could always anticipate the breach, one could always block it. Therein lies the art, and the mystery.

This is the time to change our focus from the negative (hacker) to the positive (Internet Forensics specialist) dimension of this exciting new discipline.

Conclusion

My intention here is to get you thinking about the fundamental differences between computer forensics and Internet Forensics. I think that on careful analysis, one has to conclude: these are fundamentally different skills; in the case of Internet Forensics, the skill sets of the successful perpetrator and successful investigator are pretty much the same; Internet Forensics is as much a discipline as its search-and-seizure counterpart.

The validity of these conclusions may be confirmed in any number of ways. For the most part the tools of the trade for both hacker and Internet Forensics specialist are the same, though the occasional extreme case, like Dug Song's Dsniff (monkey.org/~dugsong/dsniff/), challenges this generalization. It's difficult for me to imagine a legitimate, lawful use of Dsniff's "macof" utility that enables the users to flood switch state tables. But in the main, the hacker and the Internet Forensics specialist could coexist with the same tools and equipment.

There is also a parallel in the flow of the network traffic. Ingress traffic to the analyst is egress traffic to the hacker; the same packet-crafting technique that verifies true stateful inspection of fragmented packets also launches exploits like Teardrop and Ping of Death. Indispensable tools for packet capture and analysis, like tcpdump, are, by definition, capable of promiscuous packet sniffing, as are intrusion-detection systems like Snort. The underground hacker community and the Internet folks with the white hats are akin if one ignores the direction of their moral compass.

This is the time to change our focus from the negative (hacker) to the positive (Internet Forensics specialist) dimension of this exciting new discipline and begin to take the differences between computer forensics and Internet Forensics seriously. To make the distinction complete, we need to develop more publications on the topic of Internet Forensics, as SANS has already achieved much in the conference realm, and GIAC has established certification standards that seem to be universally accepted. If we can break from the tradition of including Internet Forensics (under some name or other) as the penultimate chapter of a computer forensics textbook and mislabeling the excellent work already done in the field under the theme of "reverse-hacking," we'll be well on our way to completely articulating Denning's durability, body of principles, body of practices, and standards for competence, ethics, and practice tests for a genuine profession.

Hal Berghel (www.acm.org/hlb) is a professor and the director of the School of Computer Science at the University of Nevada, Las Vegas, where he teaches Internet Forensics (hlb.cs.unlv.edu/syllabi/789_s03.html) and other courses in experimental networking.

Further Reading

A good introduction to computer forensics is Warren Kruse's and Jay Heiser's *Computer Forensics*, Addison-Wesley, 2002.

There are quite a few good books on Internet Forensics, though the term is not widely used—yet. Three of the best are:

- Eric Cole, *Hackers Beware*, New Riders, 2002 (www.newriders.com)
- Ed Skoudis, *Counter Hack*, Prentice-Hall, 2002 (www.prenhall.com)
- Anonymous et al., *Maximum Security, Third Edition*, Sams, 2001 (www.sams.com)

Note that the theme of all of these books is "hacking," the opposite of which is Internet Forensics. To learn one, you learn the other.

The premier password-cracking tool is L0phtcrack and its commercial version LC4. Additional information is available on the @stake Web site (atstake.com) or though a Web search on "l0phtcrack" (note: the second character is a zero).