

Stealing The Network: How To Own An Identity (2 of 3)

Discuss in Forums {mos_smf_discuss:Book Reviews}

The first two books in this series “Stealing the Network: How to Own the Box” and “Stealing the Network: How to Own a Continent” have become classics in the Hacker and Infosec communities because of their chillingly realistic depictions of criminal hacking techniques. In this third installment, the all-star cast of authors tackle one of the fastest growing crimes in the world: Identity Theft. Now, the criminal hackers readers have grown to both love and hate try to cover their tracks and vanish into thin air…

The seminal works in TechnoFiction, this "STN" collection yet again breaks new ground by casting light upon the mechanics and methods used by those lurking on the darker side of the Internet, engaging in the fastest growing crime in the world: Identity theft. Cast upon a backdrop of "Evasion," surviving characters from "How to Own a Continent" find themselves on the run, fleeing from both authority and adversary, now using their technical prowess in a way they never expected--to survive.

Chapter 7 is excerpted from the book titled "Stealing The Network: How To Own An Identity" By Timothy Mullen, Ryan Russell, Riley (Caesar) Eller, Jeff Moss, Jay Beale, Johnny Long, Chris Hurley, Tom Parker, Brian Hatch , published by Syngress. ISBN: 1597490067; Published: August, 2005

Death by a Thousand Cuts

By Johnny Long
with Anthony Kokocinski

Part 1 | Part 2 | Part 3Death by a Thousand Cuts

By Johnny Long
with Anthony Kokocinski

Part 1 | Part 2 | Part 3

Sussen was like any other small university town. Populated by academics, Sussen had its share of non-violent crime, but the sleepy town had now become the focus of a federal investigation. A local kid by the name of Charlos was struck and killed in an apparent hit-and-run while riding his bike near a local creek just outside of town. The investigation was straightforward, and local law enforcement went through the motions, but never had any reason to suspect anything other than a tragic accident despite the insistence by his roommates, a husband and wife named Demetri and Laura Neëntien, that the incident involved foul play.

The investigation into Charlos’ death was reopened a few months later when Demetri Neëntien mysteriously vanished from his home, apparently the victim of foul play. Demetri’s wife Laura was not home when her husband vanished, but reported to the investigating officers that her husband’s private journal was left open on the table. The last of its written pages had been ripped from the large book. The home was not vandalized; nothing was taken from the home except for Demetri’s cell phone and his identification, which had been removed from his wallet. The credit cards and cash from the wallet were left behind. A single spray of Demetri’s blood was found on the wall near the front entrance, but there was no sign of forced entry or a struggle.

The police declared the house a crime scene, and the Charlos case was reopened. With the help of Demetri’s wife, pieces of the story started to fall into place. It became readily apparent that local law enforcement would need to alert the feds, at a minimum. As the Feds swept in, they were appalled that so much evidence was still unprocessed from the Charlos case. Two devices, a digital camera and an iPod, were the last of Charlos’ possessions, and they were only cursorily checked for evidence. The local investigator reportedly turned on the camera, flipped through the pictures, and not finding anything interesting, returned the camera to the Neëntiens. Local investigators weren’t even aware that evidence could be found on an iPod, so that device was never even examined during the Charlos investigation. The feds sent Demetri’s journal to the lab for processing, and the two digital devices were sent to a specialized digital forensics shop.

The forensics report on Demetri’s journal revealed that Charlos had been involved with an individual known only as ‘Knuth.’ The impressions left in the journal were chemically processed, and a bit hard to read, but the resultant image was easy enough to read.

Recovered Journal Entry

The journal entry then took an ominous turn, as Demetri revealed that this ‘Knuth’ was somehow connected to Charlos’ death.

Journal Entry with Incriminating Information

After the requisite time had passed, Demetri Neëntien’s disappearance was elevated to a homicide. Demetri’s body was never found. As a result of the information recovered from the last page of Demetri’s journal, the case was marked “unsolved/pending” and ‘Knuth’ was marked as a suspect wanted for questioning in the death of both Charlos and Demetri.

Ryan Patrick’s day began like any other day in the Computer Forensics Unit. Arriving on time for work, he made his way up to the lucky 13th floor, passing all manner of varied and sundry individuals who managed to cash a State check every week without accomplishing any actual work whatsoever. Pressing his key into the lock on his office door, he turned it, pressed the door forward and slid inside, then closed the door behind him. As was his ritual on most days, Ryan managed to slip into his office without offering so much of a word of the mindless banter that required at least two cups of coffee to initiate. It felt comforting to be surrounded by the dull hum of his “FO” boxes, his Forensic Operations machines. He tapped the shift key on the two closest, FOxx and FOxy, both of which sprang to life. He had launched string searches against virtual cases the night before.

As was typical with most of his virtual cases, one string search was lagging and had not finished. This was the type of problem that kept investigators awake all night, waiting for search results for a case, which was always “the most important case we’ve ever had.” In addition to the generic search template, Ryan had added some case-specific terms to the search. FOxx had been chewing on a gambling/racketeering case and was already finished, proudly displaying a total of 130 million hits, meaning that Ryan’s added search terms were bad. Glancing at the search configuration screen, he quickly perused his search terms.

“Dirty word” searching is trickier than many people believe. Ryan had made this mistake before in an earlier case. It wasn’t that Ryan was incompetent, or that he didn’t learn from his mistakes. On the contrary, Ryan was very bright, but forensics was part art and part science, and sometimes the art got in the way of the science. During a dirty word search, the computer tries to match a specific sequence of characters. This is not the same thing as a semantic match of meaning: a technician cares about a sequence of characters in a word, but computer hard drives often contain more machine-readable code than human-readable text. Therefore an analyst must determine not only what to look for, but how to separate the human junk from the machine junk that makes up the bulk of computer evidence.

A data match that is not a semantic or meaningful match is referred to as a false positive. Ryan knew that with a number of search hits in the hundreds millions, there would be far too many false positives than he could reasonably sort through. Two mistakes were evident as he reviewed the search screen: first, Ryan had enabled only ASCII return types and not UNICODE, although this was not the reason for the high number of false positives. The custom word list was the problem.

Since this was a gambling case, Ryan had added search strings for many sports leagues, notably NFL,AFL,AL,NL,NBA and NHL. These were the strings causing all the false positives. The machine was not searching for semantic matches (the acronym of a sports league) but rather for those three characters in a row. The subject’s drive was 80Gb, and with a drive that size, the odds of any three letters being found together were high. Two-letter combinations were even more likely. Given Ryan’s list of over 20 short acronyms, the search process had dutifully found these acronyms buried in all sorts of innocent machine code on the drive. Text searching was good for data-set reduction, but only if it was used properly. With a deep sigh, Ryan checked the status of FOxy, relieved to discover that he made no such mistake on her list. He reset FOxx and, with both machines again humming away, he stepped out of his office in search of some much-needed coffee.

Ryan wandered down the hallway in the always socially-entrapping quest for caffeine. He passed by one of the six detectives in the office who was named Mike. This Mike was not as old as the other Mikes, although he had white hair and the appearance of one who had been “protecting and serving this great State since before you were another hot night for your mother, Ryan.” Assigned to the Computer Forensics Unit as the Online Investigations Officer, Mike had just been set up to start rattling of his favorite and most amusing “on the job” story. Knowing full well that his machines weren’t quite ready for him, Ryan grabbed his coffee and settled in for yet another adaptation of the famous Mike tale.

“So the chief asks if I’ve got a lot of undercover experience,” Mike began. “So I say ‘Sure, of course I do.’ He says he’s got an exciting computer job for me. So I tell him, ‘If the money’s better, or the hours are shorter, I’m your man.’”

"I show up on my first day and find out that I'm going undercover to catch computer perverts. All I have to do is sit in front of this computer all day and pretend to be a little girl in order to get the perverts to try to hit on me. I never heard about perverts like this, so I was shocked, but what can I do? I'd rather have the perverts come after me than have them go after some little girl in front of some computer. So I decide I'm gonna do my best to clean up computers to make the world safer for little kids. A few days later the chief comes by to see how I'm doing. He knocks on the door and when I unlock it and peer through the crack, he gives me this look and says, "What the hell are you doing, Mike?"

"I told him to lower his voice, and I was a bit upset that he might blow my cover, so I say "I'm undercover like you told me, Chief. Lower your voice, or the perverts are never gonna come through the computer." He pushes through the door and gives me this look. I'll never forget this look he gives me. He looks pretty mad, but eventually he says, "Mike, you know with online undercover stuff, you just have hang out online and misspell stuff when you type, right?" So I say "Sure thing, Chief, but you never mentioned anything about typing stuff."

"He looks at me again and says, "Mike, go home and get out of that ridiculous plaid skirt. And take off those goofy white knee-high socks. Are those pony tails, Mike? Did you shave your legs, Mike!?"

Mike waited for the roar of laughter to commence, then started to protest: "How was I supposed to know? It made me feel in character!" Ryan laughed with the rest of them; no matter how many times he heard that story, it was just plain funny to hear Mike tell it. On the way back to his office, Hector caught his attention.

"Heads up, Ryan: the boss is in there writing checks," Hector warned.

"Yeah? Who's getting a bad check this time?"

"Barely caught it, but I think it was some Feds."

"Glad it's not my problem," I said. "I'm already working a case."

Hector slid Ryan a look. No good ever came of a look like that. "No, Ryan. You're working virtual cases. We're all tied up fulfilling the last set of promises the boss made. Besides, you're the hotshot around here with the new stuff," Hector enjoyed the fact that Ryan was about to be saddled with another oddball case.

Ryan returned to his office, closed the door behind him, and slid into his chair. He could sense his boss, Will, at the door before the knocks he dreaded even landed. Will was fairly laid back, but slightly overanxious. He had taken it upon himself to single-handedly make a name for his shop by overextending his agents. Most places, that backfired, leaving the guy in charge holding the bag full of bad checks. But this shop was different: Will's department was staffed with young, bright, energetic talent, most of whom were single and unfettered by the responsibilities one accumulated by spending too much time in the "real world."

Will's job was to make far-out promises. And since Ryan approached each case as a personal challenge to his technical ability, he landed the oddest jobs. After a rapid-fire double-espresso "shave and a haircut" percussion riff on the door, Will pushed the door open. Sipping from one of the fifty coffee cups he used as territorial markers, Will sauntered up to Ryan's desk, invading Ryan's personal space. Ryan checked for the cornflower blue tie. No such luck.

"Ryan. What do you know about iPods?"

Although Ryan knew better, he answered on autopilot. "They're the most popular digital music player on today's market. They contain internal hard drives that can store and play thousands of songs. They have decent battery life, and are made by Apple computer, out of California. Several models are available; their sizes and capabilities vary. The high-end models can store photos as well. What else do you need to know?" Ryan wasn't sure where the marketing pitch came from, but he could already sense an incoming iPod case.

"Oh, nothing. Just wanted to make sure you knew all about them. We've got a case coming in, involving an iPod and a camera." And there it was. "I told them we could do it, no problem. I told them you were an expert."

Of course he did. Ryan knew Will. "What kind of computer is it? What's the case?"

"No computer, just the camera and the iPod. Should be here tomorrow. You're the go-to guy, so it's all yours."

“Okay,” Ryan said. “As soon as I’m done with these cases…” He turned to cast a glance at FOxy, which was still churning through his mangled string search.

“No, drop everything. This is a big deal: Feds. Double murder.” Before Ryan could even turn around or process what his boss had said, Will had already disappeared. Will disappeared with the ease of someone used to writing \$10,000 checks on other people’s \$11 bank accounts.

Ryan contacted the case agent, and asked him to fax a copy of the inventory list. Luckily, the evidence tech who seized the equipment was very thorough with the documentation of the devices: he had recorded the exact camera model, and which “generation” of iPod. The camera was not going to be a problem. He could open the camera and remove the CF card to image it in a dedicated Linux box outfitted with an 8-in-1 card reader. That wouldn’t be a problem. The iPod would be the problem.

The challenge of confronting new technology was the best part of Ryan’s job. He loved getting his hands on all sorts of equipment, and he had never actually held an iPod before. Although many forensic techs received hands-on training, to learn how to deal with new technology, Ryan had no such luxuries. Instead, he consoled himself with the notion that he preferred the process of discovery.

Whatever the technology, the key to success in an investigation, and subsequently in court, was complete documentation. As long as everything from initial testing onward was thoroughly documented on SOP exception forms, little could go wrong in court. All he needed was a third generation iPod to practice on. His bureau had no budget, and no iPods, but his buddy Scott over in the Information Services Bureau had all sorts of toys at his disposal. Ryan was in desperate need of more coffee, and now was as good a time as any to drop in on Scott.

Scott was in his office, altering a database and talking on the phone. Ryan figured he was probably talking long distance to Australia again under the guise of official business. He hovered in the door until Scott looked up. Scott immediately issued a smile and a wave-in. Ryan sat in front of the desk and looked at the bowl of M&Ms that Scott never ate, but left out for others. Ryan suspected that the candy was a distraction, aimed at keeping Scott’s visitors from realizing how long he hung on the phone.

Scott placed one hand over the phone’s mouthpiece and whispered, “What’s up?” Ryan made a small rectangle with his fingers and whispered back, “iPod.” Without interrupting his phone conversation, Scott wheeled over to a side cabinet and opened it, revealing all sorts of high-tech toys littered inside. Scott lifted three iPods out of the cabinet and held them up. Ryan looked closely before pointing at the left one, a third generation model, which sported four buttons under the tiny screen. Scott handed the unit over, along with a dock and several white cables. Ryan got up, grabbed a handful of the candy and left. Scott whistled after him; Ryan held up two fingers over his head, signaling he’d keep the gear for two days.

Armed with an iPod and its myriad cables, Ryan loaded it up with music via iTunes, then listened to it while he researched. He searched Google for “iPod forensics” and found a document that described basic forensic examination techniques. The document was very formal, and no doubt served as a forensic analysis baseline for analysts worldwide. Ryan read through the document, but was left cold by several glaring omissions.

First, there was no information about write-blocking the device. Writing to the evidence during analysis was to be avoided at all costs. If the iPod was connected to a machine, either a PC or Mac, the iPod drivers would engage, and most likely alter the drive. Ryan needed to avoid this. Second, the document encouraged the analyst to turn on the iPod and start playing with the menu (specifically “Settings > About”) to gather information about the device. This was a big problem, because the iPod was not write-locked, and the document did not explain whether or not this procedure wrote to the iPod’s drive.

In fact, just turning on the iPod might alter date/time stamps on the iPod’s filesystem. The document was a good starting point, but Ryan felt uneasy following its advice. The lawyers in the office beat him up enough to know that a decent defense lawyer could get evidence thrown out any number of ways, and Ryan wasn’t about to help out the bad guys. This left Ryan with several problems to solve. First, he needed to avoid mucking with the iPod when it booted, preferably by not booting it at all. Second, when connecting the iPod to a computer, he wanted to avoid the Apple-supplied iPod drivers, since they would probably write to the device.

Ryan needed to discover a way to bypass the Apple drivers when connecting the iPod to a computer. After searching Google some more, Ryan located procedures for entering a special iPod diagnostic mode, which would turn the iPod into a FireWire disk drive. Entering diagnostic mode and enabling disk mode would not affect the contents of the iPod. In part, this was because diagnostic mode prevented the computer from recognizing the device as an iPod, which therefore bypassed the iPod drivers.

Following instructions he found online, Ryan picked up the powered-off iPod, took it out of “hold” mode with the top switch, then held down the forward, backward, and the center select button simultaneously. The iPod sprung to

life with a whirl and presented the Apple logo. Seconds later, the device powered off. Ryan held the buttons for a few seconds longer, then let go of them. The iPod chirped, then displayed an inverse Apple logo!

iPod with Inverse Apple Logo: Gateway to Diagnostic Mode

Seconds later, the iPod displayed its diagnostic menu. Ryan cycled through the options by using the forward and back buttons until he highlighted the option labeled L. USB DISK. Ryan pressed the select button.

iPod Diagnostic Menu

The iPod lit up in red and black like an angry demon, displaying the words "USB DISK" on the screen.

iPod with USB Disk Mode Selected

Ryan pressed select again, and the screen read FW DISK, which stood for FireWire disk mode. He pressed the forward key, and the iPod rebooted. This time it displayed a large check mark with the words "Disk Mode" at the top of the screen.

iPod with FireWire Disk Mode Selected iPod in Disk Mode

Ryan had temporarily turned the iPod into a disk drive for analysis, and it was time to process the data on the drive. Ryan chose a Mac as an analysis platform, because it could handle both FAT32 and HFS+ filesystems, the default formats for Mac and Windows formatted iPods, respectively. A Windows platform would have trouble processing a Mac-formatted iPod, and Linux was a reasonable choice, but Ryan never could get the HFS+ support working well enough for forensic use. The

Mac was already preloaded with the tools that he would have used on the Linux platform, anyway; the Mac's disk image support would come in handy later, too.

With the iPod in "disk mode", Ryan was confident that the Mac would not "see" the iPod as anything but a disk drive. This would keep Apple's iPod-specific drivers from engaging, and also prevent the iTunes program from launching. Ryan connected the iPod to the Mac, and held his breath.

Within moments, the Mac launched iTunes, and displayed all of the songs he had loaded onto the iPod. "Crap!" Ryan exhaled, and fired an evil look at the iPod. Something had gone wrong: the Mac "saw" the iPod, engaged the drivers, and did God-only-knows-what to the device. There was obviously something else that was grabbing the iPod. Ryan unmounted and disconnected the iPod, then dedicated a terminal window to monitoring the system log file. After he reconnected the iPod, the system log churned out three lines, and the mystery was solved.

Apr 22 21:05:58 localhost kernel:

```
IOFireWireController::disablePhyPortOnSleepForNodeID found child 0
```

Apr 22 21:05:58 localhost kernel:

```
IOFireWireController::disablePhyPortOnSleepForNodeID disable port 0
```

```
Apr 22 21:06:00 localhost diskarbtrationd[87]: disk2s3 hfs  
0EE4323B-0551-989-BAA3-1B3C1234923D Scott /Volumes/Scott
```

The third line revealed that the diskarbtrationd process mounted the iPod on /Volumes/Scott. This was the process that handed the iPod over to the Apple's drivers. Ryan killed the process, unmounted the iPod, and reconnected it.

"I've got you now, you little," Ryan began, but the Mac interrupted him by launching iTunes again! "For the love of Pete! God Bless America!" Ryan slammed his fist on the desk so hard that the iPod jumped clean off of it. At the very least, Ryan had a penchant for creative, politically correct swearing. He stood up, scooped the iPod up into his fist, and with a face that would have stopped a train, yawped into the front of the iPod with a "Grrrrraaaaaaaaarrr!" Ryan looked up to see his boss standing in the doorway, frozen in mid-stride.

"Pretend you're me, make a managerial decision: you see this, what would you say?" Will said. He

stepped into Ryan's office, a big grin forming at the corners of his mouth.

One thing Ryan could say about Will was he knew his movie lines, and he at least had a good sense of humor. Embarrassed, but at least amused, Ryan couldn't let Will get in the last quote from one of his favorite movies, *Fight Club*. "Well, I gotta tell you: I'd be very, very careful who you talk to about this, because the person who did this... is dangerous."

Will laughed, walked closer to Ryan, and looked him dead in the eyes. He spoke in an affectless, psychotic tone, "Yeah, because the person that did that just might..." As Will spoke, Ryan watched one of the younger, more impressionable Mikes stop outside the office door, a stack of papers in hand, obviously waiting to ask Will something. "...stalk from office to office with an ArmaLite AR-10 gas-powered semi-automatic rifle, pumping round after round into colleagues and coworkers because of every piece of stupid paper you bring me..."

Will had most of the quote right, but he had mushed several lines of it together. This started one of the funniest office sequences Ryan had ever witnessed: wide-eyed, Ryan looked over Will's shoulder to see Mike still standing in the door. Mike's gaze toggled back and forth between the stack of papers in his hand and the back of Will's head. Will spun around fast enough to catch Mike tie the world speed-scurrying record, a flutter of papers the only evidence that young Mike had ever been in the doorway.

Will spun around again and faced Ryan, a look of utter shock on his face. He spun around a third time, completing an impressive 540 degrees worth of spinning, Will flew after Mike, calling, "Mike! Mike!" which caused ten simultaneous responses from the ten nearby Mikes.

"Now that was funny!" Hector laughed, his head poking up from the cube farm outside Ryan's office.

The scene was all too much for Ryan, and it took him ten minutes before he could even look at the iPod again. Once he regained some composure, he sat down looked at his terminal.

"Disk arbitration daemon," he said. "Ah... annoying."

Ryan hammered the file's permissions to all zeroes and sliced down the reincarnated daemon with an expertly-aimed kill command. With a grunt, the daemon fell, never to rise again. Ryan was lethal when he put his mind to it; in the digital world, there was no other way to describe a moment like this one. It was a battle, a fight for survival. By themselves, the commands were not that impressive, but the effect—the effect was inspiring.

Ryan jabbed the iPod into its cradle once again. This time he glared at the machine. He knew it was done right this time. He could feel it. Within seconds, his hunch was confirmed. No iTunes. No stupid drivers. It was just him and the evidence on the iPod. Now Ryan was in his element, the place where the forensics examiner ruled, the place where the enemy's precautions would fail. He connected his evidence repository disk and began by running some hashes against the iPod.

```
$ sudo -s
# openssl md5 /dev/rdisk1 | tee ~/pre_image.hash

# openssl sha1 /dev/rdisk1 | tee -a ~/pre_image.hash
```

First, he created a hash of the raw device using both MD5 and SHA1. Ryan was careful to remember the difference between raw disk device entries and block buffered device entries, and to use the `/dev/rdisk` device instead of the `/dev/disk` device. This took a snapshot of what the device "looked like" before he started mucking with it.

```
# dd if=/dev/rdisk1 of=~/.image.dd
```

Next, he created an image of the device, naming it `image.dd`. This was the file he would work from when performing his analysis.

```
# openssl md5 ~/.image.dd | tee ~/.image.hash
# openssl sha1 ~/.image.dd | tee -a ~/.image.hash
```

Next, Ryan created two more hashes (MD5 and SHA1 again), this time of the image file.

```
# openssl md5 dev/rdisk1 | tee ~/post_image.hash  
# openssl sha1 /dev/rdisk1 | tee -a ~/post_image.hash
```

Ryan created two more hashes from the iPod, to prove that the iPod hadn't changed during this extraction procedure. The process took a few hours to complete, and produced four files. The baseline hash, `pre_image.hash`, was the hash value of the device before anything was extracted. The file `image.dd` contained a bit-level disk image of the iPod. Normally Ryan would have hashed the bitstream as it came through `dd`, but this didn't work, so he skipped it.

The hash of the image file was stored in `image.hash`, and a verification hash of the original device was stored in `post_image.hash`. At this point, Ryan knew what the device looked like before and after using it, and he knew that his image of the device was correctly written to the evidence repository with no errors from source or destination.

All SOP, and each hash run through both MD5 and SHA1. This took more time, but after Dan Kaminsky raised the roof by producing very reasonable doubt about MD5, followed closely by public attacks on SHA1, every attorney in Ryan's office went bonkers. "It's the end of digital evidence as we know it," some attorney told Ryan, all but ready to resign. Ryan calmly explained that by using both hash algorithms together, one hash routine's weaknesses would be covered by the other. "Wouldn't you know, the next procedure change suggested running pairs of MD5 and SHA1 hashes on everything. Another great idea from a young attorney," Ryan thought. This was all a part of the game, and the rules had to be followed carefully, or else the bad guys walked.

Deciding on a Mac as a forensic platform in this case, Ryan changed the extension of the iPod image from `dd` to `dmg`. The Mac now recognized the file as a disk drive, which could be explored or searched after mounting it with a quick double-click. He could now browse it with the Mac Finder or run UNIX commands against it. At this point, Ryan could have a field day with the data, falling back on his solid forensic experience as he analyzed the data from the image. Since the day was nearly over, Ryan packed up his office for the night. The real iPod and camera from the field would arrive tomorrow, and he felt pumped and ready.