

Stealing The Network: How To Own An Identity (1 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 3](#)

Knuth was a formidable opponent. He was ultra-paranoid and extremely careful. He hadn't allowed his pursuers the luxury of traditional "smoking gun" evidence. No, Knuth's legacy would not suffer a single deadly blow; if it was to end, it would be through a death by a thousand tiny cuts.

It seemed illogical, but here I was: lying in a patch of tall grass, peering through \$5000 binoculars at a very modest house. The weather had been decent enough for the past three days. Aside from the occasional annoying insect and the all-too-frequent muscle cramp, I was still in good spirits.

Early in my military career, I was trained to endure longer and more grueling stints in harsher environments. I was a Navy SEAL, like those depicted in books such as Richard Marcinko's *Rogue Warrior*. My SEAL instinct, drive, discipline, and patriotism burned just as bright as they had twenty long years ago. As a communications expert, I had little problem finding a second career as an agent for the United States government, but I was always regarded as a bit of an extremist, a loose cannon.

I loved my country, and I absolutely despised when red tape came between me and tango--terrorist--scum. Nothing made my blood boil more than some pencil--pusher called me off. He would never understand that his indecisiveness endangered lives. My anger rose as I remembered. I took a deep breath and reminded myself that I was retired from the Navy and from the agency, that I had pulled the classic double-dip retirement. The frustration of the agency's politics was behind me, and now I was free to do whatever it was that Joe Citizen was supposed to do after retiring.

I can remember my first day of retirement like it was yesterday: I had never married, I had no kids that I knew of, and I puttered around my house, a nervous wreck, incompetent in the "real world." I understood at that moment what aging convicts must feel like when they were finally released from the joint. Like them, I wanted to be "put back in," forgetting how much I hated being on the inside. I grabbed for my cell phone and flipped through a lengthy list of allies, unable to find a single person who wouldn't see right through my obviously desperate post-retirement phone call.

The names flipped by, each one a memory of the many cases I had worked in my career. I stopped on one name, "Anthony." That kid was crazy, for a civilian. He was a ponytail-sporting computer forensics weenie, and despite my lack of computer knowledge, my comms background gave me a true appreciation for his work. I learned quite a few tricks from that kid. In recent years, as computers and digital gadgetry started showing up everywhere, it seemed as though I called him at least once a day.

I must have cycled through the phone's list ten times before I tossed it on my nightstand and picked up my "creds," my credentials. I opened the folded leather, to examine my "badge of honor"; for many long years at the agency, unprepared for the "RETIRED" stamp emblazoned my ID. I glanced at the

shield; I almost expected to see it too marred by my retired status. I was glad to have called in one last favor as an agent, to have opted out of the traditional plaque mounting of my credentials. I tossed the creds on the nightstand next to my cell phone and lay down, knowing full well I wouldn't be able to sleep.

The next day, while driving to the grocery store, I spotted an AMBER Alert, which asked citizens to be on the lookout for a missing child, taken by a driver in a specific vehicle with a specific tag number. As fate would have it, I spotted the vehicle and tailed it to a local shopping mall. Then I called in the alert, not to the public access number but to one of my contacts in the agency. Within moments, local law enforcement was on the scene. They secured the vehicle and took the driver into custody. The abducted child nowhere to be seen. (As it turned out, the child was safely returned to school before the driver headed to the mall.) The officers on the scene thanked me for the call. I felt a surge of pride as I presented my creds as identification. Even though I was a fed, they counted me as one of "them"; mostly because I didn't pull any of that "juris-my-diction"; crap.

Something inside me clicked, and I realized that I didn't necessarily have to leave my patriot days behind me. I still had a keen instinct for things that didn't seem right, and through my various contacts I raised federal and local alerts on several occasions. In most cases the payoffs for the law enforcement community were enormous. By avoiding the pencil pushers, I also avoided the "you're supposed to be retired, get your hand out of the cookie jar"; speech that seemed somehow inevitable.

Lying in the tall grass at the edge of a small, dense wood, I was a long way from home, and light-years away from those admittedly tame AMBER Alert tip-offs. I was looking at the home of a highly-probable scumbag who sent my "SEAL-sense" into overdrive. I was sure of that this guy was up to some seriously bad crap. In fact, I knew from the moment my brother-in-law mentioned him that I would end up right here, waiting for my moment to get inside that house. I could remember word-for-word the conversation that brought me to this particular patch of grass, and its aura of inevitability.

My family was never all that close. We all got along fairly well, but after my parents passed away, my sister and I drifted into our own lives. Our visits eventually dwindled down to holidays and special events. At a recent holiday gathering, I had a chance to chat with my brother-in-law Nathan, a good-hearted small-town electrical contractor. Nathan and I were from two completely different worlds, but his easy manner and laid-back attitude made him approachable and easy to talk with, and I enjoyed our too-infrequent conversations.

"Naaaytin! Long time!" I called out as he walked into my house. I was eager to have a conversation that consisted of more than "It's been way too long."

"Hey, stranger! How's retired life?"

I was genuinely impressed that he remembered. "I can't complain. The pay's not too bad"; I said, trying to mask the fact that I was completely miserable with my new existence. "How's work going? Anything exciting happening out there in the sticks?"

"It's been a good year, actually. I picked up quite a bit of extra work thanks to our own local eccentric."

"Really? An eccentric? You mean the 'building bombs in the log cabin'; type of eccentric?" I couldn't help myself.

"Yeah, I can tell you're retired," he said with a laugh. "No, this guy's harmless. He's just different. He's just rich, and he likes dumping his money into his house. I mean he paid about \$300k for the place, and as best as I can tell he's dumped another \$350k into it, most of it paid in cash."

"What? \$650,000 in cash? That's absurd!"

"Well, it wasn't cash, exactly, but from what I hear from the local realtor he didn't secure a mortgage. That's her way of saying he paid the house off early."

"He must have really expanded that house for \$350,000. It must be the biggest house in town by far."

"Not really. Like I said, he's eccentric: he spent a lot of money fixing up the basement. From what I hear, he bought steel plating for the downstairs, which he framed out for some sort of bomb shelter or something. He had a big A/C unit placed on a new slab in the back, with ducts that fed only the basement, and I installed a monster generator pushing 60 amps at 120 volts, 60 hertz, with a large gas tank pushing backup power to just the basement. Like I said, not a big deal, just sorta strange. I made decent money on that, so I can't complain."

"Steel plating? A/C units, backup power? That is a bit strange. Any idea what the guy does for a living?" I

hated pumping him for information, but something didn't seem right about this picture. This 'eccentric' seemed wrong somehow.

'Nobody knows for sure. Some said they heard he was a day trader, which explains all the communications lines he had run.'

'Communications lines?' Now Nathan was speaking my language. I knew comms.

'Well, from what I hear, he's got around \$1500 a month worth of Internet and phone circuits going to the house. The guy has more connectivity than the rest of the town put together.'

Something didn't feel right about this guy; the whole situation just felt wrong. If what Nathan was saying was true, this guy was up to no good. The steel plating would serve as a decent shield against electromagnetic fields. In com-speak, that room was 'Tempested'. This meant that snoops would be unable to monitor his electronic activities while in that room. The power, A/C and com lines all added up to some serious redundancy and tons of juice for a small fleet of computer gear. This

guy was no day trader, that was for sure. This guy was paranoid, and from the sounds of it, he was rich. At the very least, he was probably running some sort of junk email operation; at the very worst, this guy was into... God only knew what. The only thing that didn't fit was the way this guy spent his money. spam kings, tech moguls, and even successful day traders tended to live lavishly. This guy, on the other hand, kept a low profile. I had to get more details without Nathan thinking I was too interested in this guy.

'Well, who knows? Every town's entitled to at least one eccentric,' I began. 'I bet he's got nice cars, a monster TV, and all sorts of other cool stuff too. Fits that rich, eccentric sort of profile.'

'No, he drives a pretty beat up truck, which he only uses to haul stuff from town. And trust me: there's no room in that place for a big TV. He's a recluse, like some kind of hobbit or something. That's what makes him mysterious and eccentric. He doesn't come out of his house much. From what I know, he hits the local general store every now and then, but other than that, no one ever sees the guy. Ah well, enough about him. I feel sorry for the guy: he's all alone. With that short cropped hair and large build, he's probably ex-military. Probably took a nasty ding to the head while he was in the service or something. I don't like to judge folks. Besides, like I said, he paid well for the work I did, and for that I'm grateful.'

Short military cut? Large frame? Recluse? I didn't like the sound of this guy one bit. My sister interrupted my train of thought. 'Now that you're retired,' she said, 'you're out of excuses.'

I shook my head, startled by my lack of environmental awareness. Somehow my sister had managed to slip next to her husband without me noticing. Tunnel vision. I couldn't have gotten this rusty already. 'Excuses?' I asked.

'Whenever we invite you for a visit, you've always had some excuse. It's been too long. Why don't you come stay a few days? You've never even seen the house. Nathan wants you to visit, too.' She shot her husband an elbow to the ribs.

'Oh! Sure, man! Me too. It would be fun,' Nathan bumbled, obviously startled by his own enthusiasm.

I had to admit: I was out of excuses. The country air would do me good, I knew that. I needed a change of scenery if I ever hoped to have a real retirement. 'You guys don't need,' I began.

'We want you to visit. Seriously. Besides, we're the only family you've got left.'

She had a point. I knew she was right. 'Sure, I'd love to visit for a few days. Won't you guys be busy with work?'

'Sure,' Nathan said, 'You would have quite a few hours to yourself, and we could spend the evenings together.' Nathan sounded genuinely enthused about the idea.

'Okay, okay: I give in. I couldn't help smiling. 'When should we...'

My sister interrupted. 'Next week. You know as well as I do that if we put it off it won't happen.' She was right.

'Okay. Next week it is.'

When I returned home, I packed a few clothes. Out of habit, I tossed my tactical field bag into the trunk, too. It wasn't a short drive, but it wasn't long enough to warrant a plane trip. Besides, I still felt naked without my sidearm, and I didn't feel like dealing with the hassle of airport security goons.

My sister and her husband put me up in a guest bedroom, and although I was alone for a large part of the day, it was nice to spend time with them in the evenings. After a few days, however, I had drained their pantry pretty severely. Remembering the general store I passed on the way into town, I decided it was time for a road trip.

Pulling into the gravel parking lot of the store, I remembered Nathan mentioning something about a general store during their last visit. "The Hobbit," I said out loud, surprising myself. I had all but forgotten about the local eccentric.

The store clerk was an unassuming woman named Gretchen who had a very easy-going way about her. I felt completely at ease as I introduced myself. As I checked out, I asked her a few questions about the local eccentric.

I learned that the Hobbit always drove his beat-up truck, never walked, always bought strange rations like soup and bottled water, and had been gradually losing weight and growing his hair and beard. The fact that he was changing his appearance was a red flag to me. As I asked more casual questions about the town, my mind was made up: I needed to get more info on this guy. If nothing else, he was socially odd. My curiosity had the better of me.

I returned to my sister's home and fired up her home computer to do a bit of research. After plugging through lots of searches, including property records, I was left empty-handed. This was going to require a bit of wetwork. At the very least, as long as I had my gear packed in the trunk, I could watch him for a while. That evening, I let my sister and her husband know that I was planning on taking a few day trips. They seemed happy to see me getting out and about. I didn't like lying to them, but I couldn't exactly let on that I was coming out of retirement.

I was extremely cautious as I settled in to monitor the Hobbit. I scoured the perimeter of his house for any sign of detection devices. Finding none, I installed my own: I wired the perimeter with various electronic sensors to alert me when something was amiss at any of the property borders or the major driveway junctions. The range of my sensors allowed me to receive alerts from a great distance, but even so I spent several hours a day monitoring the house from various discreet vantage points. One thing I knew very well was the "sneak and peek" and unless this guy was a fellow SEAL, he wouldn't know I was around. I occupied vantage points far beyond the Hobbit's property line, but well within range of my doubled 4Gen AMT night vision binoculars.

The Hobbit poked his head out only twice in nearly a week. Once, early in the week, he drove to town to get some scant rations and vitamins. The second time he came out of his house, something was very different: first, he paced his entire property line in what was an effective (yet seemingly non-military) sweeping pattern. He was very obviously looking for signs that he was being monitored. He didn't find any of my gear and, obviously satisfied, he disappeared into the house, not to emerge again until dawn the next morning.

After his perimeter sweep, I knew Hobbit was planning on making his move. I stayed on surveillance until dawn the next morning, when I was awakened by a sharp constant chirping in my earpiece. Alerted by the familiar alarm, I slowly and deliberately scanned the perimeter to find Hobbit walking down the road towards town. This was it: he was on the move. He had no bag and, given that no one in town had ever seen him walk any reasonable distance, let alone the hour-plus walk to town, I was sure he was leaving for good. As he passed out of distance, I retreated through the back side of the property line, charged through another set of properties, and hopped into the driver's seat of my car, winded.

With a ball cap pulled down low over my eyes, I drove down the town's main access road. I spotted Hobbit walking away from me, nearly a half a mile down the road leading towards town. Since it was just after daybreak, I had a very good view of him, and decided to stay way back until he was out of sight. He never once turned around. He was a cool customer, and he didn't raise any suspicion to the untrained eye. He was just some guy out for a walk, but I already knew he was on a one-way trip.

After nearly an hour and a half, he reached the Greyhound terminal. Watching from a long distance through the binoculars, I saw him approach the ticket agent, presumably to buy a ticket. I got a glimpse of the bus schedule through the binocs, noting that the next bus left for Las Vegas in about 45 minutes. Hobbit was at least 45 minutes from leaving, and was a solid hour and a half walk from his house. This was the break I needed: I had a small window of time in which I could get inside his place, see what was what, and get back to the bus station to tail this guy. I turned the car around and headed back to Hobbit's house.

I parked outside his property line, and walked across his property. I collected all of my sensors and pulled on my gloves as I made my way to the house. I had no reason to suspect that there was anyone else inside the house, but I wasn't taking any chances: my personal SIG-Sauer P226 9mm sidearm was at the ready, loaded with Winchester 147 grain Ranger Talon jacketed hollow point rounds. My constant companion through my years as a SEAL, and an approved firearm for my agency details, the weapon felt right at home in my grasp—even though I had no

business carrying law enforcement rounds and a concealed weapon as a civilian.

As I rounded the windowless side of the house, I approached the garage door and, finding it unlocked, proceeded into the garage. "Federal Agent!" I called instinctively. The words sounded foreign to me, and I decided against formalizing my entry any further. I swept the house, instinctively cutting the pie in each room. Discovering that I had the house to myself, I began to take a closer look at each room, beginning with the garage.

A large gas generator was installed here, and from the looks of the installation, the main grid power fed through it, into the ground, and presumably into the basement. A smallish furnace was here as well, next to which lay a crucible, a large sledgehammer, and a pair of molds. The furnace vented out through the garage wall, and curiously enough, no vents ran from the unit to the house. This furnace was certainly not used for heat, begging the obvious question. The sledgehammer was nearly new and, despite a few minor paint scratches, looked as though it had hardly been used.

Parallel scratches on the concrete floor indicated that several rectangular metal objects, each approximately three inches by five inches, bore the brunt of the sledgehammer's fury. Tiny shards of green and black plastic and bits of metal were scattered around the floor. The glimmer of a small dented Phillips-head screw drew my eyes to a broken piece of an immediately-recognizable IDE connector. I wasn't much of a computer geek, but I knew what a hard disk drive looked like, and these were chunks of hard drives. Since all of the drives' large pieces were missing, I could only assume that the Hobbit had been melting everything down in the furnace, pouring the resultant glop into the molds, and passing off the useless hunks of sludge in the weekly trash pickup.

This was my first confirmation that Hobbit was up to something. If Hobbit was a harmless ultra-paranoid, he wouldn't have thought to invest the time and resources to melt down hard drives in order to protect his secrets.

Walking across the garage, I came to an odd-looking sander mounted on a small bench next to what appeared to be a bin full of CD-ROM discs. Upon closer inspection, I noticed that the bin was filled not with CDs but rather with the remnants of CDs: their reflective surfaces were all scuffed off, which left only a pile of scarred, transparent plastic discs.

A small bin next to the shredder caught my eye. I peered into it, mesmerized by the miniature, sparkling desert wasteland of sanded CD "dust" that I discovered inside. This little contraption sanded the surfaces off of CD-ROM discs, which made them utterly useless. Hobbit was smart, and he was the definition of an ultra-paranoid. Whatever he was up to, I was pretty sure there would be no digital evidence left behind. I glanced at my watch. I needed to bail in about twenty-five minutes if I had any intention of following his bus.

The rest of the rooms on the first floor were empty and rather inconsequential. One room contained a LaserJet printer, various network devices, and a pair of PC's, cases and hard drives removed. I flipped open my cell phone and instinctively speed-dialed Anthony's cell number.

"Yo, retired guy," Anthony answered before even one ring.

"Got a quick question for you, and I'm short on time."

"Uh oh. Why do I get the feeling you aren't doing normal old guy retired stuff?"

"We'll talk in hypothetical terms then," I said, knowing full well he had already seen through my current situation. "Let's say a suspect melted down all his hard drives and shredded all his CD-ROMs. What would be the next thing to go after?"

"We can reassemble the CDs. No problem."

"Good luck. The CDs are transparent coasters and a pile of dust."

"Did you say dust?"

"Dust, Anthony."

"Big flakes or little flakes?"

"Dust, Anthony. Look, I'm a very short on time here, and if I don't get out of here…"

"Woah, you're just as crotchety as I remember. OK, OK, so no hard drives, no CDs. What else is around? Digital stuff, electronics, anything."

"Well, I've got two rooms. In this room, I see a hub or a switch, a pair of LaserJet printers, a cable modem, and two PC's minus the hard drives."

“Well the first thing my guys would look at is the cable modem. Depending on the brand, model, and capabilities, there could be good stuff there. Unfortunately you’ll need proper gear to get at the data, and some of it’s volatile. You’ll lose it if the power drops.”

“Sounds complicated.”

“That’s why the feds pay us the big bucks. You mentioned LaserJets. What kind of LaserJets?”

“An HP LaserJet 4100, and a 3100.”

“Hmmm… look in the back of the 4100. Any option slots filled? They’re big, like the size of a hard drive.”

“Nope. Nothing. Looks empty.”

“No hard drive unit. That’s a shame. Still, there may be jobs in the printer’s RAM, and we should be able to grab an event log with no problem, so don’t go mucking with anything. If you start spitting test prints out of those printers, you might nail any latent toner that’s sitting on the transfer drum.”

“Transfer drum? Kid, I don’t know what you’re talking about, but if you’re telling me I can’t so much as dump a single page out of these printers, I’m gonna wring your…”

“Woah! Easy there! Man, I’m glad I’m not a terrorist if this is how you talk to people trying to help you! All I’m saying is that if you print anything, you could clobber any chance we have at hard evidence if this thing happens to turn up on our case docket.”

“Fine. No printing. Got it.”

“What’s the model of the other printer?”

“LaserJet 3100.”

“A LaserJet 3100? Hmm… Let me see…” I heard Anthony typing as he investigated the model number. “HP…LaserJet… 3100… Oh! That’s an all-in-one device: fax, scanner, and copier. If the fax has anything cached, that might be useful. Again, don’t go printing stuff, but you might be able to get some info by poking through the menu with the buttons and the LCD screen.”

“Buttons and LCD screen? This sounds utterly useless to me.”

“What do you expect? The guy destroyed all the good stuff.”

“He left behind the rest of the PCs though. Can’t we get anything from the leftovers?” I was fuming that Hobbit was smart enough to nuke the drives. I knew that hard drives contained the bulk of digital forensic evidence found on a scene. I was sure we were screwed without those drives.

“Well, I’ll be honest with you. I’ve never run into a problem like this. I’ll have to ask around, but I think we can get the lab to pull stuff off the memory chips or controller cards or something with the electron microscope. But this guy’s going to have to be tied to something big to get that gear pointed at him. I’ll have to get back to you on that one. I hate to say it, but I think you’re screwed on the PCs. Any USB drives, floppies, anything?”

“Nope.” I had that sinking feeling again.

“O.K. What else you got?”

“Well, that’s it in this room. Now the next room…” I said. “We’ve got more.”

As I entered the second of the basement rooms, my cell phone disconnected abruptly. I glanced at the phone’s screen and saw that my phone was out of service. I backed into the other room and redialed Anthony.

“Joe’s Morgue. You bag ‘em we tag ‘em. Joe speaking.”

“Anthony? Sorry about that. There’s similar stuff in the other room. More gutted PC’s, a Cisco box,

a couple of hubs, and that's it."

"Well, the Cisco is going to be a good potential source of data, and maybe those hubs. Something does seem strange about a guy that melts his hard drives, removes all his media, and destroys the rest. Who is this guy, hypothetically?"

I thought about the question for a second. "He's a scumbag. I just know it. He's up to no good. Isn't it enough that he's rich, reclusive, destroying potential evidence, and an ultra-paranoid who's high-tailing it on a Greyhound bus?"

"Not really. You've just described half the suits working in the D.C. corridor, except for the Greyhound part. Anyhow, you better watch yourself. You're a civilian now. If there's a case, you could get all this evidence tossed in court. Besides that, you could get locked up for..."

"Look," I interrupted. "This guy's into something big. I don't have time to go into the details, but my instinct's never been wrong before. Look, I gotta go. I've got very little time here. I'll call you back in a bit, but for now keep this under your hat. Please."

"Sure. Just remember: if this turns into more than just your little retirement game, we're going to need every last speck of evidence, so do us all a favor and tread lightly. You were never there. Otherwise this case turns into a mess in court."

"Fine. I read you... Thanks, Anthony. Out."

I hung up the phone, glanced at my watch, and realized I was short on time. I headed over to the first of the printers, the LaserJet 4100. After poking through the menus, I realized that uncovering anything of any consequence required that I print a report. There were some interesting looking reports available, such as "PRINT CONFIGURATION" and "PRINT FILE DIRECTORY," but I had to rely on the kid's advice. Keep it simple, and keep it clean. I did, however, find that I could view the printer event log with the LCD screen by selecting the "SHOW EVENT LOG" option from the Information menu. The output of the event log seemed useless, as I didn't understand any of the information it displayed. I shifted my focus to the other printer, the all-in-one LaserJet 3100. As with the other printer, most of the informational reports such as "FAX LOG," "TRANSMISSION REPORTS," and "PHONEBOOK" seemed to require the device to print, which I couldn't do. One menu item, "TIME/DATE,HEADER" looked safe.

LaserJet 3100 Configuration Menu

Using the buttons and the LCD screen, I could see that the fax machine's phone number was set to 410-555-1200, an obviously bogus number.

Fax Phone Number Configuration: Obviously Bogus

Another item in this menu revealed the header info for outbound faxes contained the phrase "KNUTH INDUSTRIES."

Fax Header set to Knuth Industries

"Knuth," I said to no one.

None of the background research I had done on this guy mentioned anything about a Knuth. I had checked property records, public records, general background, and had even run a LexisNexis SmartLinx search with my federal user account. Still, nothing about "Knuth." This was possibly the first name or alias this guy hadn't purposely made public. It could very well be the piece I needed. I glanced at my watch. Time was wasting. I had fewer than five minutes to get out of Knuth's house, or I risked missing that Greyhound bus. The rest of the equipment in this room was useless without mucking with anything.

I walked into the second basement room and glanced around to make sure I hadn't missed anything obvious. This room, like the other, was completely barren of any obvious evidence. There were no paper scraps, no notebooks, no USB drives, not even so much as a blank pad of paper or a pen. I could only assume that anything of interest has been incinerated. In fact, seeing how meticulous this "Knuth" was, I realized that the entire place had probably been wiped for prints. Without a doubt, this was the most meticulously cleaned home I had ever seen in my life, and it was the most forensically barren scene I had ever witnessed. God help the forensics team that would work this scene. I left the second room, prepared to leave. As I ascended the stairs, my cell phone chirped into service. I had forgotten that my cell phone disconnected earlier, while I was talking to Anthony.

“I wonder,” I thought aloud. I looked at the LCD screen of my phone: three bars. “Decent signal for a basement,” I mumbled.

I continued to watch the screen as I walked around the basement. When I entered the second room, my signal disappeared. Nothing. Out of service. As I backed out of the room, my cell service returned within seconds. I decided to give room two another look. The only thing even slightly odd about this room was the odd-looking cover over the A/C vent. As I stepped in again to take a closer look, I remembered the steel plating my brother-in-law mentioned. This was the steel-plated room.

Knuth had built himself a very nice Faraday cage, and all it housed was a small collection of computer equipment. This guy had crap for machines. He wasn't a day trader, he wasn't a tech mogul, and he wasn't some sort of SPAM king—at least not with this crappy gear. This guy wasn't technical in nature. If he was, he would have nicer gear, and the whole “digital” lifestyle. Knuth was using his computers to commit a crime. I was convinced, even though a tiny percentage of the population is equally paranoid without also doing anything illegal. Statistically speaking, anyone living like this was up to something. Leaving everything as I had found it, I left the house and headed for the station.

I parked my car a good distance away from the Greyhound station. Wielding my binoculars, I was relieved to see Knuth waiting in line to board the Vegas-bound bus. I dialed Anthony on my cell phone. He answered before the first ring again.

“Hey. What's up?”

“I've got a potential name and a destination. Think you could put up a flag in the system for me, in case there's some info on this guy?” I knew I was pushing my luck: I was asking the kid to do something that could get him in trouble.

“Look, I don't mind putting it into the system. It's not as if I've violated his due process in this thing. The fact is that eventually you're going to have to explain how you got this information, and that's where things get ugly. You do realize that if your hunch is right, you could land yourself in prison, or worse: you could be helping this guy get off because of what you're doing right now.”

“You don't think I've thought of that? Look kid, no offense, but I've faced tougher battles than this in my career. I've crawled through…”

“Your career is over,” Anthony interrupted. “Based on what you've told me, though, this guy is up to no good. Give me the info, and I'll toss it in and see what squirts out. It's your ass… not mine.”

“The name is Knuth. Kilo November Uniform Tango Hotel. Destination is Las Vegas via Greyhound, bus B8703. And thanks, Anthony.”

“Don't thank me. Thank Bubba. I'm sure you two will be very happy together in your new cell.” The kid had a point, but if my hunch was right, no lawyer in the world would be able to save Knuth.

Sunshine. The Pacific coast had it in abundance, and it would take Blain some time to adjust. He was not at all used to the sun; he spent the majority of his time indoors, as evidenced by his pale complexion and his constant squint when venturing outdoors. Tall and thin, Blain wore inexpensive glasses and sported blonde hair that looked shabby from every angle. Looking for shelter from the sun, he ducked into the next building, which was labeled ED04. According to the map, crossing through this building would dump him right next to PHY02.

Blain grabbed a pen from his backpack and wrote this building's number on his hand. He was sure that he would make further use of its shade as he traveled across Pacific Tech's campus. He slipped the pen back into his backpack, hefted the bag onto one shoulder, and looked around as he walked.

With the exception of one active computer lab, this building was relatively empty. It seemed completely devoid of students.

Before his first Physics class next week, he had to check the status of the equipment in the PHY08 lab to ensure that the room had sufficient materials and equipment to conduct the class's experiments. He had thoroughly read the entire semester's worth of assigned text and felt fairly confident that he could make a good impression by helping the professor out with some of the obviously basic exercises.

Although the majority of his first semester's classes seemed well beneath his skill level, Pacific Tech offered the best program for his intended double major of Physics and Computer Science. Beyond that, he had followed the work of one student in particular, and had come to idolize him. Mitch Taylor was at the forefront of the field, a real genius in his

own generation. The mere thought of meeting Mitch convinced Blain that Pacific Tech was the school for him. His mind made up, he filled out an application and was accepted in short order.

Blain pushed open an exit door. Squinting, he pressed on towards two buildings, one of which was PHY02. His eyes were still adjusting to the sun as he strode to the next building, pulled open the door, and ducked inside. Almost immediately, he came to a flight of steps leading down to the basement level. Hearing voices and mild commotion downstairs, he bounded down the stairs in his typical two-steps-at-a-time style, hoping to ask for directions.

As he bounded down onto the landing, his foot slipped out from under him. As he tried to correct himself, he spun, his backpack flew off his shoulder and lofted through the air, down the hall. Blain was still spinning and in motion, horizontal and three feet in the air. He heard a voice yell "Bag! Duck!"

Completely disoriented, Blain smacked into the wall. Then, landing on his back, he thudded onto the floor and slid face-up down the hallway, until he smashed into the opposite wall. Finally he stopped, face up, a tangle of blonde hair and lanky limbs in the middle of the hallway.

A quick diagnostic revealed no breaks or contusions, and as he parted his hair from his eyes, he saw two faces bending over him, one male and one female. The male had dark hair and dark eyebrows, and he looked to be the age of a high school junior. He clutched Blain's backpack by one strap, having caught it mid-air as it sailed down the hallway. The cute and brainy-looking female looked over at the young man, glanced at the backpack dangling from his clutch, and said "Nice reflexes!"

Turning her gaze back down to Blain, she asked "Are you okay?"

Dazed and confused, but unhurt, Blain managed a smile. "Sure."

Standing in the doorway, backpack still in hand, the high school kid offered Blain a hand. "Here," he said, "it's easier if you try to stand up in here."

Refusing any assistance, Blain scooted into the doorway and stood. He snatched his backpack and unceremoniously pulled it onto his back, tightening both straps indignantly.

"Ooh, I left the acetate in the microwave," the girl said, "I've gotta go." Gently touching the high-schooler's hand, she stepped out the doorway and slid gracefully down the hall.

"She was a cutie," Blain thought to himself. "What's going on here?" he asked, irritated.

"A small test. I can't say exactly, but it's a frictionless polymer," the guy answered with a smile.

"And it spilled?"

"Not exactly."

"Did you make it?"

"I'm not saying, but I can tell you that it's fairly rare, and very unstable."

"Who's cleaning this up?"

"It doesn't need cleaning up. In a few minutes the oxygen in the air will neutralize it, turning it into water."

"Whoa." Irritated and embarrassed about his acrobatics display, Blain had completely forgotten the Physics lab number he was looking for. He dug into his pocket to find the slip of paper he had scrawled on earlier. Pulling his hand from his pocket, he opened it to find his keychain and the slip of paper that read "PHYS08."

"Can you tell me where the PHYS08 lab is?"

"Wrong building. Next one West."

"OK. Gotta go."

Blain spun on his heels, forgetting all about the unbelievably slippery floor just behind him. He stepped quickly into the

hallway and lost his balance almost instantly. Refusing to go down a second time, he thrust his arms out to his side in the universal "balance" position and, in doing so, rocketed his keychain from his right hand. From down the hallway, he heard a voice yell "Keys! Duck again!"

Blain twisted his body so he could see the direction his keys were going. As he did so, his feet spun, which again put him off balance. Not traveling far this time, he landed sideways in a crumpled pile, somehow having slid into the room just across the hallway from where he began his goofy ballet. Indignant, he scrambled to his feet. Blain raised his gaze across the hall, where he saw the familiar male standing, arm outstretched, Blain's keychain dangling from his fingertips. "You okay?" the young man asked. Glancing at the keychain, he said "Wi-Fi detector. Nice, but there's no wireless on campus. It's policy." He tossed the gadget back to Blain. "You must be new here. Why else are you looking for the Physics lab on the weekend?"

"I just want to get there and check out some stuff in the lab, make sure that the materials are sufficient. Then I need to find the computer labs. I'm just afraid that this school is not going to have adequate equipment. I heard that the computer labs here have single processor machines with only 512MB of RAM. How can anyone learn on that?"

"I think they are fine. I did okay."

"Sure, for the basic user. But my stuff is going to need more power. I'm sure of that. I'm a Physics and Computer Science major."

"Oh, so what are you working on?"

"Don't worry about it," Blain said. "Some say it is master's thesis material. I'm sure you wouldn't get it."

"Sure."

"Thanks for the directions. I gotta go."

"Sure thing." The high schooler paused. "Oh, by the way, my name's Mitch Taylor. These days everyone calls me Flir."

"You're Mitch Taylor?" Blain looked like he was going to get sick. "The Mitch Taylor? Oh no."

"Oh yes!" Mitch smiled.

"I... there... computers... and then Chris... freeze the... Argon!" Blain didn't look so good. His entire system fully engaged the "flight" portion of his "fight or flight" instinct and, with all the coordination he could muster, he speed-shuffled down the hallway, nearly falling twice, and headed back up the stairs that he had come down moments before.

After three days of searching for Mitch, Blain thought, he had finally found him. And then he launched his loaded backpack at Mitch's head, hurled his keychain at him, insulted his intelligence, and made himself look like a complete fool, all in the span of five minutes. He couldn't have felt more stupid. Blain hurried back to his dorm room, shattered.

It was late on Saturday night, and Blain couldn't sleep. Since his run-in with Mitch, he had trouble concentrating. His sullen and ill-tempered attitude wasn't making a great first impression on his roommate. Fully dressed, he got up from his bed, pulled on his sneakers, grabbed his ever-present computer backpack, and pulled it on. Blain slid out his door, closing it gently behind him. It seemed as though the Pacific Tech campus never slept, but at this time of night it was quiet. The night air was doing him some good. As he walked around for what must have been a solid hour, Blain realized that he had been focusing too much on the incident with Mitch.

"I'm certainly not the first person to make a bad impression," he thought aloud, "and I won't be the last."

As he rounded the corner to the ED04 building, Blain stopped as he saw someone who looked like Mitch entering ED04. "He's probably making his way back to his dorm," Blain thought. Seeing this as a sign, Blain decided to take this opportunity to apologize to Mitch for being such a jerk. He picked up his pace toward the building, rehearsing what it was he would say to Mitch.

As he pulled open the door to ED04, he was surprised to see that Mitch was nowhere in sight. From his vantage point

and current trajectory, Mitch should be straight ahead, near the exit, on his way through to the dorms. Blain kept constant pressure on the open door and silently eased it closed behind him as he padded into the building. The building was empty as always, but Blain could hear the distinct sound of a chair sliding across the room in the computer lab ahead. He froze in his tracks as he heard another sound from the computer lab: the sound of a desk sliding out of place.

“Now that’s odd,” Blain thought to himself. “Why would he be moving the desk?”

Frozen in the hallway, Blain listened. Although he couldn’t explain why, he couldn’t move. Something felt odd about Mitch’s behavior, and his timeframe. He glanced at his watch: 1:22 AM. The next sound was the oddest of all, and Blain recognized it immediately. It was the sound of duct tape being pulled from the roll. This sound repeated several times.

Blain realized how odd he must look, standing there in the hallway like a deer in the headlights. Without making a sound, he sidestepped into a room to his left, across the hall and down from the computer lab. Although he was not in sight of the lab, he could still make out the sound of lots of duct tape being expended. By the time the taping stopped, Blain was convinced that an entire roll had been used. Next came the familiar sound of a sliding desk, followed by a sliding chair. The faint, sharp sound of a zipper told Blain that the person in the lab was finished and was leaving. As he heard the sound of footsteps, Blain had a moment of panic: he would be discovered, standing like some kind of stalker in the door of the classroom. He held his breath and sighed quietly as he heard the exit door lever engage at the opposite end of the hall. Peering around the corner, Blain saw Mitch, backpack over his shoulder, leaving the building. Mitch had been in and out in less than 20 minutes, but to Blain it seemed like an eternity.

Blain had forgotten all about his plan to apologize to Mitch. Instead, he was consumed with intense curiosity. He felt a sharp twinge from his conscience, but he summarily ignored it, knowing full well that he had to find out what Mitch was up to in that computer lab.

Convinced that Mitch was long gone, Blain emerged from the classroom and made his way to the computer lab. He had no idea what he was looking for, but he knew that a chair and a desk had been moved, and that Mitch had expended a lot of duct tape. Blain worked his way from desk to desk, and looked under each and every one, but found nothing out of place. Thinking for a moment, he realized that the sounds suggested Mitch might have been taping something to the back panel of a desk, where it would remain unseen from the front. Blain was consumed by his curiosity, and continued his search. Eventually he found what he was looking for, stuck to the back of the desk farthest from the door, completely encased in black duct tape, network and power cables extruding from its wrapping; a laptop. Mitch, or “Flir,” as he said he was known, was up to no good. “Flir,” he thought out loud, “is a hacker handle if I ever heard one!” Blain snickered to himself. “I have to get access to this laptop.”

Blain knew that Flir might be using the laptop remotely, so he tucked the desk back the way he had found it and left the lab, heading towards the dorm buildings. Only a handful of rooms on the ground floor had lights on, and he walked towards Flir’s window, which he had scoped out after his unfortunate incident. He could hear the unbelievably loud sound of power equipment inside, and as he peered through the window, he saw the cute girl he had seen earlier with Mitch. She was in the center of the room using a circular saw on what appeared to be the top frame of a car! Mitch sat off to the side, a pair of headphones on his head as he fiddled with an aluminum can and several wires. Blain recognized the equipment immediately, and realized that Flir was building a “antenna,” a low-cost wireless antenna. Blain had little time, but knowing that Flir was busy in his room gave him the confidence he needed to get to work on Flir’s laptop in the lab. He ran as fast as he could back to ED04, and sat down at the far corner desk, winded.

The first order of business was to dismount the laptop from the bottom of the desk. Removing all the duct tape took a bit of work. It was important to remove the machine so that it could be returned to its position without Flir noticing that it had moved. This frustrating job took nearly 10 minutes, but once the machine was removed, it was easy to flip open despite the huge layer of duct tape still attached to the top of the machine. Blain took a closer look at the machine, a very nice and brand-spanking-new Sony VAIO. It was a shame to see such a nice machine coated

with duct tape.

“Your grant money at work,” he thought with a grin.

The duct tape on the back panel bulged slightly. Three Ethernet cables and a power cable protruded from under the duct tape near the bulge. The power cable connected to the power strip under the desk, and (based on the information printed on the power adapter) powered a small hub. One of the Ethernet cables connected to the VAIO’s built-in Ethernet port. The second cable connected to the classroom LAN, and the third cable plugged into the lab computer that sat on top of the desk. This simple configuration tapped the workstation’s LAN connection, and provided wired access to both the lab machine and the laptop. Connected to the laptop was a USB wireless interface; a cable ran from the adapter’s antenna jack to the back panel of the laptop, underneath the duct tape. Blain assumed this was a flat patch-style antenna. That explained Flir’s antenna project.

Although it was a bit of a chore, Blain managed to open the laptop. As he expected, he was greeted with a black screen with white letters, prompting him for a username. "Linux," he said out loud.

At this point, Blain had a bit of a dilemma: in order to keep tabs on what Flir was up to, he was going to need to get into this machine. Grinding through default usernames and passwords seemed meaningless, as Flir wouldn't make this classic mistake. He flipped through each of the consoles, making sure there wasn't a console already logged in. No such luck. Blain knew that his best bet was to boot the machine off his USB drive loaded with Puppy Linux, which he always kept in his bag. If he was able to boot the machine from the USB stick, he could mount the laptop's hard drive and insert himself a nice backdoor.

Blain opened his bag, grabbed the USB stick, and pressed it into the VAIO's USB slot. He wondered if Flir would notice the reboot. Although he was pretty sure that Flir hadn't yet connected to the laptop, he held his breath and bounced the box. Within a few seconds, the machine rebooted, and Blain tagged the F3 key to try to enter the BIOS setup. His heart sunk when the machine prompted him for a password.

"I need to get into the BIOS so I can boot off this USB..." Blain said to himself. Then a thought occurred to him. He looked through his bag, and within seconds he produced a CD-ROM from the CD wallet he always carried in the bag. The scrawled label on the CD-ROM read "Knoppix Linux 3.8." Knoppix was a CD-based Linux distribution that had gotten Blain out of a jam on more than one occasion, and he hoped this would prove to be another such occasion. He opened the drive tray and slid in the CD. Holding his breath as he rebooted, the seconds seemed like eternities. Blain nearly jumped out of his chair when the Knoppix boot screen displayed on the laptop.

"YES!" Blain shouted, forgetting for a moment that he was trying to keep a low profile.

When Knoppix booted, Blain logged in, unset the HISTFILE variable to prevent logging, and mounted the VAIO's primary partition:

```
# fdisk -l

Disk /dev/hda: 40.0 GB 40007761920 bytes

Units = cylinders of 16065 * 512 bytes

Device Boot Start End Blocks Id System
/dev/hda1 * 1 4863 39062016 83 Linux

# mkdir /mnt/tmp

# mount -rw /dev/hda1 /mnt/tmp
```

This gave Blain access to the laptop's file system. Next he created a script on the laptop that would create a root user and set its password when the system rebooted.

```
# echo "echo bla:x:0:0:bla:/:bin/sh >> /etc/passwd; echo bla::::::: >>
/etc/shadow; echo bla123 | passwd bla &dash;stdin > /etc/rc3.d/S98f00f"
```

After rebooting the laptop, Blain logged in as the "bla" user. His first order of business was to look at the password file, to determine the user accounts that existed on the machine. The only user account of interest was the "kent" account. There was no telling how many Kents were on campus, but there was little doubt that Flir was poking fun at Kent Torokvei, a local geek bully Flir loved playing jokes on. He knew it was a waste of time to attack passwords on the machine, since he had shell access, but decided to snag a copy of the rogue's password files just in case it became necessary.

Blain looked at his watch and realized that he had been sitting in the lab for nearly an hour. Although no one had entered the lab since he arrived, he could easily be mistaken for the owner of the rogue laptop. It was time to get some monitoring software in place and get out before someone discovered him. He needed something sexy, something quiet. The perfect tool came to mind; sebek, a data capture tool designed by the researchers supporting the HoneyNet Project. A honeypot is a networked computer that exists for the sole purpose of being attacked. Researchers install and monitor

honeypot systems in order to learn about the various techniques a hacker might employ. Once a hacking technique is known, it becomes easier to create an effective defensive technique. Although this sounds like a fairly straightforward process, it can be quite a challenge to monitor an attacker's knowledge. This is where the sebek tool comes in handy. Designed to be very difficult to detect, sebek keeps tabs on the attacker's keystrokes via the kernel's `sys_read` call, and sends those keystrokes across the network to a sebek server, which displays the keystrokes for the administrator who is watching. Blain needed to install a sebek client on Rogue, and a sebek server on his own laptop. He pushed the client up to Rogue, and began configuring its options.

Blain set the interface (`eth1`), the destination IP, and destination MAC address in Rogue's sebek client install script. These settings ensured that the monitoring packets would be sent from the proper interface on Rogue and that they would be sent only to the IP and MAC address that matched Blain's laptop. Setting the `keystrokes only` value to 0 ensured that the client would collect not only keystrokes but other data as well, such as the contents of `scp` transactions. Blain executed the `sbk_install.sh` script on Rogue, thereby installing and executing the sebek client. At this point, any keystrokes, and all other `sys_read` data, that occurred on Rogue would be covertly sent out from Rogue's wireless interface to Blain's sebek server, which would also be listening on his laptop's wireless interface. It was a rather elegant setup, allowing wireless monitoring of the hacker without an established connection to the machine, bypassing any encryption the hacker might be using when connecting to Rogue. Before launching the server, Blain made a few quick modifications to the `sbk_ks_log.pl` script, which displayed the hacker's keystrokes. Having used sebek before, Blain had no use for details like date and time stamps, so he removed them from the program's output. With the client installed on Rogue, Blain launched the sebek server on his laptop.

```
sbk_extract &ndash;i eth1 | sbk_ks_log.pl
```

To test the setup, Blain typed a single command into Rogue's shell, the `ls` command. Almost immediately, his sebek server on his laptop burped up a single line:

```
[2.3.2.1 6431 bash 500]ls
```

The sebek server output showed five fields. First was the IP address of the rogue's wireless interface, `2.3.2.1`, followed by the process ID, and the name of the command shell (in this case `bash`). Finally, sebek reported the command shell's arguments, in this case the `ls` command. The monitor was in place. Now the only thing Blain could do was wait for Flir to make a move. Blain thought for a moment about installing a backdoor on the device but decided against it, knowing that Flir might get spooked if he found something glaring.

“No,” Blain mumbled, “keep it simple.” Blain returned Rogue to its position under the desk. Satisfied that the machine was in its original hidden position, he gathered his belongings and headed back to his dorm to get some sleep.