

Course Review: SANS FOR408 Computer Forensic Investigations – Windows In-Depth

By Jason Andress

The field of forensics used to be the ugly step-child of the ethical hacking world. In fact, it wasn't even in the InfoSec category at all for the longest time. It was a realm populated by one of two types - the lonely IT guy hired by law enforcement to handle general tasks or the unlucky law enforcement officer who admitted that he knew something about computers. My have we come a long way. Not only is there now multiple disciplines, network forensics and file system forensics, but also each has its own sub-specialties for a given technology. Thus file systems forensics break into mobile and desktop varieties, and further areas of specialization for OSX, Linux and Windows. And with any maturing industry, there are a slew of training options available.

The SANS FOR408 Computer Forensic Investigations – Windows In-Depth class covers the needed skills for proper forensic acquisitions and analysis of devices with this operating system. While many classes focus largely on forensic acquisitions and on a single or just a few tools, FOR408 goes into great depth on the analysis side and covers a multitude of tools: some pay and some free, some open source, and quite a few that will make the hair stand up on the back of your neck. The class also plumbs the depths of a number of operating system artifacts that lurk in the crevices of Windows and is generally a great deal of fun for the forensically-minded. This course and review is slightly different, as I attended the SANS vLive version of this class. Let's take a look at the specifics.

Discuss in Forums {mos_smf_discuss:Andress}

Upcoming SANS vLive Forensics Courses

vLive FOR408

Computer Forensic Investigations & Windows In-Depth

Begins March 18

vLive FOR508

Advanced Computer Forensic Analysis and Incident Response

Begins March 19

vLive FOR610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Begins March 28

\$150 Off with Coupon Code: EHN_Connect

Before the Class

While the class itself certainly constitutes the meat of the material in this review, I would feel remiss as a reviewer for not talking about the bits beforehand. Having had previous experience with SANS On-Demand classes, and having had books for such classes shipped to me previously, I was a bit surprised when a somewhat larger-than-usual box arrived on my doorstep. Inside, as shown below, were the typical SANS books that I expected, as well as an additional bag of gear for performing acquisitions from storage media.

Being a somewhat stereotypical geek in this regard, I immediately set aside the books and opened the bag, therein finding a Tableau write blocker and all of its associated cables, adapters, and other such goodies. I haven't included a picture of the gear itself, as this would need to be an aerial photograph, but you can see the inventory list from the bag below. It's always a good start to a class when you get new toys to play with.

Lab Setup

Also included in the box were two course DVDs containing the VMware image for the class, various tools, materials for the labs, materials for the final day challenge, as well as instructions for setting up the image and VPN connection.

The only hitch for the entire course (and a minor one) was due to the licensing of the SANS Investigative Forensics Toolkit (SIFT) image. As I had previously read in the course requirements online, students are required to provide a retail Windows 7 Home Premium license key in order to run the SIFT kit image. As I have a license for Microsoft TechNet, I had every expectation of being able to grab a key from there and be good to go. As it turns out, the very week before I tried to get said key, Microsoft removed them from the TechNet library for new downloads. As I had not previously downloaded the key, I was not able to get one this way. Through a bit of sneakiness on my part (details not included to protect the innocent), I was able to get the image up and converted to Windows 7 Professional, for which I had a proper license. Several other people in the class had the same issue. Other than this, the remainder of the lab setup and VPN configuration (you need this to talk to the license server for some of the pay tools) went flawlessly, all of this being documented in multiple places, as well as thoroughly discussed by the instructor on the first day of class. This is, however, a process that I would suggest going through in advance.

Editor's Note: SANS is now providing a Windows license to every student as part of the course to resolve the issue.

Day 1

This was my first experience with a SANS vLive class. As I understand it, the format is generally the same across the various classes offered in this format. The class met twice per week at 7:00 PM Eastern time and ran for three hours over a total of 12 meetings. So each group of two classes is roughly the equivalent of one day in an in-classroom SANS class. The course tool is a web conferencing tool called Elluminate which offers text chat for the students, audio from the instructor, and a main window to view the slides or other tools that the instructor might be sharing on the screen. Overall, the tool was just fine, and there were no issues with it for me throughout the entirety of the course. The view of the course window can be seen below.

The instructor was Chad Tilbury, a 12-year veteran (in both senses); first of the forensic and computer investigations field and also a former Special Agent in the Air Force Office of Special Investigations. It's always nice to get an instructor for a class that has a good body of experience with their topic, as they generally have a good set of stories to tell. This was absolutely the case here. Chad was a great instructor overall and had a very deep set of technical knowledge in general and was chock-full of helpful tips and instruction when it came to the tools and process that the course covered.

The first day of the class saw 32 students, and Chad mentioned that the size of the forensics classes keeps increasing. He also mentioned that a 13% job growth in the forensics field over the next couple years is expected.

We spent a fair amount of time during this class going over the lab environment on the virtual machine (VM) and did a high-level overview of some of the included tools and how to configure the VPN in order to talk to the license server for the pay tools to which we were given access.

Topics covered in this class were a bit of a primer on forensics in general, such as how to work with the SIFT Kit VM, forensic investigation methodology, fundamentals of gathering and handling evidence, and a bit on evidence acquisition. My favorite bit for the evening covered memory acquisition and analysis. We ended up with a lab on performing an acquisition with FTK imager.

As a side note, when we wrapped up with starting the lab, I worked ahead a bit and got it done before the next class. I would definitely suggest working ahead a bit on the labs. The class is very fast paced, and doing so allows you a bit more time to digest the material, recover from mistakes, and have questions ready to ask the instructor next time.

Day 2

The second class started out with a discussion on evidence issues in the case of one of the 9/11 bombers, Zacarias Moussaoui. We also talked about how there are no NIST "officially approved" forensic tools, only tools that have been tested. Following was a discussion on hash algorithms (such as MD5, SHA, etc.). Forensic forums routinely debate what should be used in court, but to dispel any myths, we looked at a case where the FBI successfully defended the use of a 32 bit CRC to verify evidence integrity.

We spent a bit of time at the beginning of the class going over the labs that the previous class ended on. As I mentioned before, this went rather quickly, and I would suggest working through them in advance.

This class consisted almost entirely of evidence acquisition, largely centered on the use of FTK. The highlight of this class for me was the use of the Tableau write blocker kit included with the class to acquire an image from a hard drive. This is another place where reading the course requirements comes in handy, as you are expected to provide your own media on which to perform the acquisition.

We finished up the evening with a discussion of the Windows file system, covering topics such as slack space, file system metadata, how the file system has evolved over time, timestamps, etc.

Day 3

We launched day three with a discussion of the Donald Blake case. This is the case on which the majority of the examples and exercises for the rest of the course are built. I won't give too much away on this so as not to spoil the surprise, but in short, Donald is an employee who was fired and may have committed a bit of intellectual property theft on his way out the door. I really liked the scenario as it allows the various examples and tools for the course to fit into a more cohesive framework rather than just developing individual examples as they were needed.

Topics for this class included an introduction to the Donald Blake case, an overview of the FTK toolkit, and string searching and data carving. I particularly enjoyed the data carving discussion and being able to recover some of the deleted items from the Donald Blake case was quite a bit of fun. One of the most enjoyable pieces of forensic analysis for me is being able to come behind the folks that have taken measures to delete files or destroy data and being able to almost immediately discover and recover it.

This class finished up with a hands-on exercise on using keyword searches in FTK to locate specific data in the large mass of data that you may find at hand. This is definitely a very handy skill when searching through large bodies of data.

Day 4

We started this class out with a cautionary tale about a police detective who accidentally wiped all of the data from a Blackberry mobile device due to carelessness and poor use of tools. This led to a bit of a discussion on both mobile device forensics and the importance of safely handling media or devices that contain the original copies of the data with which we might be working.

This class was spent almost entirely on the subject of email forensics. We discussed client and server-side email investigations with common environments such as Microsoft's Exchange and Outlook tools, as well as how we might investigate the use of webmail and a bit on email on mobile devices as well.

We finished up the class with a particularly enjoyable lab which had us searching through a .PST file (from MS Outlook) in order to trace back to the source of several spam emails, all of which required both the use of the appropriate tools and a bit of detective work.

Day 5

Day 5 started out by going over the spam lab from the last session and working through the process to find the required information. We also discussed an interesting court case involving the Motion Picture Association of America (MPAA). During the case, the court ordered RAM dumps to be obtained from servers which were located outside of the US. These servers were being used to house bit-torrent files of copyrighted materials and were specifically configured to not keep logs of the activity regarding the torrent files. Needless to say, the RAM dumps provided fully adequate evidence for the court case to proceed.

The material for this class started out with a discussion on E-Discovery, largely from a legality and process standpoint. From there, we jumped right into Windows registry forensics. The registry forensics section was, for me, one of the high points of the entire class. Sure, most of us who have been around a bit have worked with the registry, know where some of the interesting bits are, and have fooled around with changing some key values, but this material is on a whole other level. From a very high level, we covered a bit of the general registry overview as well as covering information on how users and groups are laid out in the registry.

Day 6

Day 6 started off with an interesting (and perhaps somewhat less digital) discussion about a suspect in a murder investigation. The person in question, who had claimed to be nowhere in the vicinity of the murder in another state, was found out due to the nature of the insects that were stuck in the radiator of a vehicle that he had rented, insects that were local to the area of the murder. While this may seem to ultimately be unrelated to the topic of digital forensics, it was a very nice opener for finding location specific information stuck in the Windows registry, such as the names and/or IP addresses of wireless access points that are local to a specific area.

This class continued on with registry analysis, moving on to system configuration and analysis of user activity. The really interesting bits were the odd information and level of detail on various user and OS goings-on that get stored in the registry. This is the point in the class where you really start to get creeped out and paranoid about what your computer is remembering about you. This section of the class managed to be both enlightening and uncomfortable at the same time, a difficult combination to pull off, let me assure you.

We finished up the class with a lab involving the use of a few different tools to pull interesting information out of the registry. This is an area in which you truly rely on the tools in order to be able to parse the interesting bits out of the massive volume of data that this present.

Day 7

Day 7 started out with the tale of a USB drive which contained quite a large amount of medical data. To make matters worse, not only did the device hold medical data, but criminal data for the patients as well. This discussion was an excellent opener for the section of registry analysis that dealt with tracking the activities of USB storage devices.

Again, as another somewhat uncomfortable but very interesting topic, in this class we delved into the analysis of USB activity through the use of information stored in the Windows registry. As it turns out, tracking the exact devices use, computers to which they were attached, who was logged in at the time, what was moved to or from the device, and a number of other interesting and related bits, are a relatively trivial matter. This is another place in the class where, from an investigative standpoint, I had a bit of an "Aha!" moment and learned quite a few new things about the use of USB devices under Windows.

We finished up the day with a discussion on people swallowing removable media such as USB sticks and memory cards in order to avoid being caught with damaging evidence. As it turns out, and just for future reference, such media will generally survive the trip through a human digestive system relatively unharmed and perfectly readable.

Day 8

Day 8 started off with a discussion about our instructor Chad working with a former student who had a case of IP theft by an employee that had left the company, and how this oddly paralleled the Donald Blake scenario.

This class launched us into the topic of Windows artifact analysis in which we covered link files, jump lists in Windows 7, Microsoft Office and media file metadata, analysis of thumbnails, the Windows recycle bin, and prefetching. File and document metadata having long been a personal interest of mine, I found the section particularly interesting. I especially appreciated the dive into EXIF data for media files and the use of ExifTool, as I don't often see these covered well in such classes.

Day 9

Day 9 kicked off with a discussion on 4 US Army Apache helicopters in Iraq that were destroyed (to the tune of \$16 million each) due to exposure of geo tag information in a picture posted on the Internet.

This class finished up the prefetch discussion of Windows artifact analysis and started off with log file analysis. In discussing log files in the Windows environment, we went over the basics of event logs and event log analysis, which you might expect to not be the most interesting material in the world. However, we did touch on quite a few topics that spiced things up a bit, such as searching for evidence of malware, tracking down rogue accounts, and looking for suspicious services. Event log analysis is a very easy place to become overconfident, but the casual user is only scratching the surface of what is actually there.

Day 10

We started Day 10 by talking about new chips for mobile devices that can specifically pinpoint altitude in addition to coordinate data to add an additional layer of specificity to positioning information.

This class finished up the event log discussion from the previous class and launched into browser forensics. The browser forensics material in this class is absolutely top-notch. We spent quite a bit of time discussing the information that you can see in the browser itself (cookies, bookmarks, cached files, etc.), and how that differs from the huge load of material that tools built for browser forensics can dredge up. One topic that I found particularly interesting was the discussion on what exactly the private browsing mode that has become a common option in the last few years for the major browsers actually does. As it turns out, private browsing mode doesn't really do all that much to protect you. Hordes of data is still created by your browser and written to your storage device. Once again, one of those interesting places in the class where you realize how much you really don't know about what your operating system is doing in the background.

Days 11 and 12

Day 11 started out with an hour or so of wrapping up browser forensics then launched into the capstone for the class which continued into Day 12. I won't go into any great detail on what the final effort for the class is, as I don't want to give away any secrets or ruin the surprise for anyone, but suffice it to say that it is a great deal of fun. You have the option of tackling this yourself or working as a team, whichever appeals to you. The task involves applying all of the skills and tools from the whole course to solve the mystery, as well as properly documenting and reporting what you found.

Wrapping Up

Overall this was a great class. I had a good time, which is always a bonus, got to play with new and interesting software tools, and even got a bit of hardware out of the deal. Chad was a great instructor and very knowledgeable, told interesting stories, and was full of great information and helpful tips all the while.

I haven't taken the GIAC Certified Forensic Examiner (GCFA) exam associated with the class yet, but will be sitting for it in February. I'm busy indexing and tabbing the books presently, and will be going back through all of the labs to make sure that I have the tools down. I will also be reviewing the next SANS forensics class in line, FOR508: Advanced Computer Forensic Analysis and Incident Response, so look for a review of that coming down the pipe as well.

Dr. Jason Andress (ISSAP, CISSP, GPEN, CEH) is a seasoned security professional with a depth of experience in both the academic and business worlds. In his present and previous roles, he has provided information security expertise to a variety of companies operating globally. He has taught undergraduate and graduate security courses since 2005 and conducts research in the area of data protection. He has written several books and publications covering topics including data security, network security, penetration testing, and digital forensics.