Computer and Network Forensics: A Masters-Level Curriculum
Transcript

Part 1: What a Student Can Expect: Practical, Hands-on Experience

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally-funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Shownotes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT, working on operational resilience and software assurance. Today I'm pleased to welcome back Kris Rush, a member of CERT's Forensics Team. As a side-note, we've posted two previous podcasts on forensics that you might want to listen in on, to get a little background. And today Kris and I will be discussing a new forensics and incident response track that Kris and his colleagues are now offering through Carnegie Mellon's Information Networking Institute. It's become part of the Master's of Science in Information Networking degree program. So we're going to be talking about that today. So welcome back Kris, glad to have you with us.

Kris Rush: Thank you. Glad to be here.

Julia Allen: So why did CERT decide -- I mean, you guys have been working in the forensics area for some time now. But why did you decide that now was a good time for codifying everything that you've learned and experienced into a graduate level curriculum in forensics? And maybe just a little bit about how you went about developing the curriculum.

Kris Rush: Sure. Well we've been doing this for about the past five years. It started out a little slow. A few staff members here at Carnegie Mellon and CERT focused on the forensics mission; primarily with the outreach and development of some educational modules for the customers we had. And then eventually that transitioned into us being called on to help with law enforcement and the (U.S.) federal government with solving some of their more difficult forensics challenges. And so that's how our mission has expanded. And we're continually being called upon to provide expertise in some of the more challenging areas and to solve some of the new problems that investigators are coming across as they pursue investigations.

And so where that really led us was -- with one of our missions being outreach and education, in addition to this operational support -- we realized that there wasn't a great central place for people to get this education. And we realized that Carnegie Mellon, being a fabulous technical school, that it only made sense for us to make some effort to provide a program where after completing it, students would have the ability to perform forensic investigations from either a law enforcement perspective, whether or not they were integrated into an enterprise or a business. And so we've really decided to take some of the lessons learned, just the general lessons learned, as well as some of the harder problems that we've encountered over the past several years, and to transition that into course work that the students could take away some actual concrete skills that they could apply in a job beyond education.

Julia Allen: So if I was going to be a student, first of all what would you describe as the ideal background coming into this curriculum? And when a student comes out the other end, what might they be able to do?

Kris Rush: Well there seems to be a lot of students that are attracted to the forensics field, both students and professionals. And we find that there is no single common background, other than a general interest in computers. I think that the curiosity about computers is what really drives people towards forensics.

And so typically most of the students will have somewhat of a computer background, with varying degrees of technical capabilities. So some people may have more of a network management, enterprise management slant to their past experience, while others are more oriented with programming and some of the more technical tasks in that regard. And so what these people get out of it are different based on how they come into the program.

What everybody walks away with is a general understanding of the fundamentals of computer forensics, and what it means to be a forensic investigator or a forensic analyst, and to actually take forensic casework on, or investigations on, and to do a good thorough job and find all the information there is to find.

Where it really differs with what they leave with is the program is structured in a way that students can tailor the outcome to their own abilities. Beyond the core fundamentals, people with a more technical expertise and more defined technical interests, may walk away with the ability to actually develop new tools, to develop new techniques, and to actually begin furthering the field of computer forensics. And that's the sort of people that we actually really like to see come out of here, because we know at the end of that student's time here at Carnegie Mellon that we've had an impact on them, and that potentially they will have an impact on the forensic community.

And the other students, which walk away with equally useful skills, are ones which may not want to go into the deep technical programming tools or actually tackling new, really difficult challenges in the field of forensics, but walk away with a complete understanding of how to conduct a forensic investigation, down at the disk level, without tools. And that's a really concrete, hard to learn skill as well.

Julia Allen: Well I'd like to drill down a little bit into some of the course curriculum and, so our listeners can have a better appreciation of some of the details that you and your colleagues have put together. So from the Carnegie Mellon Information Networking Institute website, at least I was able to find five courses in the track. And so what are those five? If you would just briefly introduce them, and then we can talk about each one in a little more detail.

Kris Rush: Sure. So you're right. Right now there are five. And the idea behind that is we established five which would form the core curriculum of the program. And beyond that we would ideally be adding smaller special topic courses that would sort of supplement some of the more robust and difficult challenges that you can't really tackle while you're also tackling 12 other things, through the course of a single class.

So the five that we've currently got on offer are: Host-Based Forensics; a follow on to that, which would be Advanced Host-Based Forensic Analysis. Then we move into the network field. So we've got a Network Forensics course; an Advanced Network Analysis course. And then finally we're offering an Event Reconstruction and Correlation course.

Part 2: Host-Based Forensics

Julia Allen: Okay, so why don't we start at the top. In the Host-Based Forensics, both the introductory and the advanced, what are some of the dimensions, problems, course projects -- the kind of things that students will be exposed to and have to dig into?

Kris Rush: Sure. Well the Host- Based Forensics class is really, at the highest level, exactly what it sounds like. These are centered around challenges and skills required to perform a forensic investigation on a single host; whether that be looking for information that was inappropriately accessed; whether that's a machine that's compromised as a result of malware or some other form of computer attack. There can be a lot of reasons why one might want to undertake a specifically host- based analysis. In a more corporate environment, this sort of be -- could fall along the lines of e-discovery or understanding sort of what files existed on a computer.

As far as what the course specifically looks at, it really is a soup to nuts look at what is required to conduct a host-based analysis. And so that goes into everything from the planning of what's required to conduct that investigation; what pieces of evidence you need; how you want to go about acquiring that evidence (all the planning phases around that); what you do with the evidence once you have it; how you keep it clean and secure, and make sure you're working with appropriate copies.

We look at acquisition challenges. So there's your standard “how do we acquire a forensic image of a disk coming out of a computer?” -- through some of the more difficult challenges that one might face in trying to acquire a forensically sound image of a computer.

One of the bigger chunks is spent on the actual analysis. So we're looking at computers and what's resident on the disk for pieces of evidence that may support either a law enforcement investigation or that would support some action to be taken by an enterprise or a business. Like I said, this could be a lot of things. In the law enforcement realm, you'd be looking for things that were contraband-like material -- whether that be illicit images or credit card numbers. Find evidence of types of malicious code living on a machine that may have been developed there; things along this line as well as other standard evidence -- proof of identity theft; proof of access to confidential information belonging to an organization. All things of this type.

And then we really go into the reporting. Because we feel that even if you've got the technical skills, one of the key requirements of this is that you be able to convey what it is you found in a forensic investigation to someone who may not be as technical as you, or as technical as your colleagues, so that they can understand what it is that you found and how that relates to the investigation at hand.

Julia Allen: Do you find, in this particular course and probably in the network course as well, do you teach students how to interface with law enforcement? So if you're a network or system administrator and you're involved in a forensics investigation, is one of the dimensions of the course where does the organizational role and responsibility dovetail or integrate with that of law enforcement, if you're actually going to get law enforcement involved? Do you get into that?

Kris Rush: We spend a fair amount of time in one of the prerequisite courses -- which is Applied Information Assurance, which is the precursor to all of these courses -- discussing the legal framework for computer forensics. That would entail the capturing of logs; the capturing of network traffic; how to handle specific events; when it may be appropriate to involve law enforcement. So yes, we certainly do spend some time with a focus on that. A lot of our work is

in the law enforcement arena, but we really tried to formulate a course that is rather agnostic to the terminology or the handling of data and evidence. But yes, students do walk away with a sense of when it would be appropriate to involve law enforcement; how to maintain the value of evidence, and the integrity of evidence, if you think you might be turning it over to law enforcement; things of that nature.

Julia Allen: Great. And what about the advanced course, the companion to Host-Based Forensics? I know you get into special topics there. Are there some particular ones you'd like to highlight?

Kris Rush: Well the advanced course is really an opportunity for us to highlight and to teach and convey some of the more unique challenges. And the idea behind the Advanced Host-Based class is that we'll change this every so often, as new challenges come on the scene and as we're able to present new ways to tackle those. For instance, some of the things that we've been looking at currently in the advanced classes involve things like data carving, manual data carving. A lot of people will rely on tools and whatnot to do data carving and to find elements of files that may exist in deleted space on a disk. This is an opportunity for students to spend a fair amount of time in real-world scenarios, actually carving up a disk and piecing back together elements of files that have been found in unallocated sectors.

Some of the other interesting stuff that we're looking at is small-scale digital devices. A lot of traditional digital forensics has focused on either cell phones, in particular, or actual computers. Well, as I'm sure you're very much aware, a lot of the things that we deal with in this day and age really contain computers, or elements of computers, and data is stored in a lot of different ways, across a lot of different devices. And so one of the challenges that we're presenting in the advanced course is what are some of the devices that may yield potentially useful forensic evidence? How do we get it? Is there work previously done in this field, say something like GPS devices? What work has been done, and are there ways that we can create new tools or new techniques to get even better information out of these types of devices?

Julia Allen: And I would imagine that also the advanced course, on both the host and network side, as you said, give you an opportunity that if there's some trend line or some new tooling or new form of investigation or some new attack strategy, that the advanced courses provide an opportunity to keep the students fresh, right?

Kris Rush: Exactly. And that's why we created some of the advanced courses, and why we'll create some of the other courses, is because it's very difficult to have a fluid, semester-long course that deals very much in fundamentals. And so while we can bring up those topics in those courses, it's really difficult to present to students really in-depth challenges that involve quite a bit of concentration without having these special topic courses.

Part 3: Network Forensics

Julia Allen: So Kris, let's move on to the Network Forensics and its companion advanced course. What kinds of topics and techniques and approaches might students be exposed to in the Network Forensics course?

Kris Rush: Sure. Well the general Network Forensics course concentrates on actually several topics; some which may not seemingly be tied directly to network forensics. We looked at the ones that you'd expect to see, like collection of network evidence and the analysis of evidence associated with any sort of network forensic event. We were looking at things like netflow for statistical analysis, to identify behavioral characteristics of traffic, as well deep packet inspection

to understand the actual behavior of any given session and understand what say an attacker or an individual is trying to do across the network.

Another thing that we've found seemed necessary in this track was to actually look at malware analysis. Very rarely does a piece of malware not rely on the network. And there's a lot of information that can be gleaned by performing both static and dynamic analysis of malware, in order to figure out what the intention of the malware was; what affect it may have had on your network; what can you go back and look at in terms of logs to see any another anomalous behavior that you may have expected. And from a law enforcement perspective, it can really lead you to sort of that next hop. So outside of your organization, where did that attacker come from or where did that piece of information that was exfiltrated go? And so that's one of the important things that we felt was critical to highlight.

And then we also looked at some of the more standard stuff you might expect to see -- like how do you actually capture the data off the network; and what the implications of various collection methods might have on the types of data that you'll collect from different types of collection.

Julia Allen: Well what if you don't have access to the network though? As you're well aware, these attacks and scenarios and incidents can be global in their nature. So how do you teach students to deal with the fact that key parts of the transaction that resulted in the forensics investigation may be missing?

Kris Rush: Sure. And so this is actually one of the areas where potentially -- if you look at it through a corporate lens versus a law enforcement lens -- your ability to affect this process may be different. So in a law enforcement perspective, you have more ability to reach out to other vendors, other providers, even potentially to other nations, and potentially try to track down those involved in a potential computer crime. And so your scope there tends to be much larger.

And from a corporate perspective, we realize that these are challenges that they do face, and that they do not have access just as the law enforcement would. And so what we still try to teach though is that if you're looking at a corporate case, or if you're looking at a business that calls a law enforcement agency and has a concern, there's a lot that can be gleaned even from network traffic collected on your own network.

A lot of malware relies on the network to either continue attacks, to further attacks, to spread, or to exfiltrate data. And so by looking at the network for these types of behaviors, you can glean a lot of information about your investigation -- including things like what was trying to be exfiltrated? What sort of services were being exploited? Were they actually successful? Is it potentially a case where we have other incidents of this malware running on other machines across our network or across our enterprise?

So there are a lot of instances where even though you don't have access to that global set of data, or even the ability to reach out to it, you can still glean a lot of information.

Julia Allen: Excellent. Well that's very helpful. Thank you. And obviously there's a companion advanced course that goes with the network side as well. So what are some of the special topics that you're kicking around or are showing up in the content for the advanced course?

Kris Rush: Sure. So this one really does differ a little bit from the original Networks Forensics course. This course is really focused on dealing with traffic across large networks. One of our understandings is that a lot of people that leave Carnegie Mellon, with this specialty degree, aren't going to be in law enforcement. They're going to be working in business environments.

And as such, typically in these cases, you're not just a forensic investigator. You're also looking at network traffic. You're handling incidents across networks. And we thought that it would be critical to actually give people some skills so that they could conduct these activities and have experience in doing this.

So some of the stuff that we're looking at in this course is, like I said, large network traffic collection and aggregation; large-scale analysis of network and packet data for any anomalous behavior or potentially malicious activities. So not just from a single investigative perspective, looking at a series of sessions related to an attack, but when you're attacked -- looking at network across a large organization or enterprise -- how do you identify those specific anomalous events, or how do find things that may be malicious and need further investigation? And that's really where this course differs from the general Network Forensics course.

Part 4: Event Reconstruction and Correlation; Student Feedback

Julia Allen: So the last course of the five, at least as you currently have it constructed, is called Event Reconstruction and Correlation, which obviously by its nature is putting data together. So what kinds of things do you introduce students to in that particular course?

Kris Rush: So event reconstruction is really one of the essential elements to the program. It's aimed really to enable students to conduct a soup to nuts complete forensic investigation. And this one's a mixture of both lab and lecture. And it gives the students the actual opportunity to tie together a lot of the components from the other courses, into an actual full-scale investigation. So this is really their chance to figure out in their own way how to combine these multiple facets of digital forensics and draw a single conclusion regarding an event or a law enforcement case.

Julia Allen: I assume then you actually give them cases and they work on small teams and have to present the results of their efforts.

Kris Rush: Yes. We're currently working on building examples and scenarios of cases that we actually have familiarity with -- and some of the more advanced and difficult cases -- which recreating those in a full-scale is often a very difficult task. But we're trying to present to them an array, a myriad of evidence that they would have to deal with, mixed in with pieces of evidence that aren't that important, and having them actually conduct full investigations, or several full investigations, over the course of a half a semester.

Julia Allen: Excellent. So I know this is the first year that you and your colleagues have been offering the curriculum. So what are some early indicators that you're seeing in terms of student response, feedback, success? Any early results that you'd like to share with us?

Kris Rush: Like I said, this originally got its roots in the Applied Information Assurance course, which I believe has been taught for about four years now by several of our colleagues. And we realized through that course -- which was very unique at the time, a blend of lecture and actual hands-on labs. And then we saw that there was a real strong need for those types of courses. Because a lot of times at this level in education students are very much introduced to concepts but they're not introduced to a practical application of those concepts; and that tends to be a problem. These people are not going out and writing white papers. They're actually going out and controlling networks and they're responsible for security of large enterprises or for handling massive incidents. And we found it to be a really critical thing that when they go out there into the world and are tasked with these things, that they have some insight as to how to do these things. And so based on the success of that course, and the number of students that we saw taking it, we realized that not only from an information assurance perspective, but from a

forensics and investigative perspective, students would really appreciate the ability to both be introduced to the concepts -- which is the standard, typical type of education students get at the master's level -- but to walk away also with concrete skills that they could apply and they could put on their resumes and walk out the door and be immediately applicable in the field.

And so, so far what we've seen is that students are very pleased. I think students are surprised sometimes with the level of breadth, and with the depth as well in the curriculum, as well as the standards to which they're held to. These students are -- at the concept level you write a paper and sort of eek your way by. But these are things where students are expected to deliver actual results and to solve actual problems.

In some of the advanced courses, these students are expected to actually conduct real research and present new ways to solve problems. And I think that students are really intrigued by the idea of having an effect on a larger community and walking away with a pretty unique set of skills.

Julia Allen: Well it sounds like you and your colleagues are creating a very rich educational experience, and I'm hoping that in addition to sending these folks out to do good things in their organization, we can take advantage and hire a few of them ourselves.

Kris Rush: That was one of the reasons that we saw a need for this. We do incorporate a lot of students into some of the projects that we undertake here, just to pursue new opportunities and new ideas. And we did find that as we were bringing them in, very few of them, even at the advanced degree level, had some of the more fundamental understanding and basic skills required to work in the field of forensics. And so that was very much an impetus for wanting to do this.

Julia Allen: Excellent. So in addition to the INI website, and other websites that describe the curriculum Kris, do you have some pointers where our listeners can learn more about just the general subject area?

Kris Rush: Sure. Our website on the CERT website, for the Forensics Team, has quite a bit of information regarding some of the publications that we've made in the past, as well as some of the achievements that we've had, as well as access to some of the curriculum and more specific topics that we've addressed.

Julia Allen: Excellent. Well my hat's off to you. I think you guys are definitely laying the groundwork for the profession and the improvement of the profession, and also giving us an opportunity to codify and package and communicate so much of what you and your team have learned. So I really do thank you for your time today.

Kris Rush: Well thank you very much Julia. I was very pleased to be here.