Just Digital Forensics Program Development and Outlook

Introduction [00:00:05] Now this is recording RTI International Center for Forensic Science Presents Just Science.

Voiceover [00:00:19] Welcome to Just Science, a podcast for justice professionals and anyone interested in learning more about forensic science, innovative technology, current research, and actionable strategies to improve the criminal justice system. And Episode three of our Strengthening the Forensic Workforce Season Just Science sat down with Dr. Mark McCoy, professor and administrator of the Digital Evidence and Cybersecurity Program at the University of Central Oklahoma Forensic Science Institute, and Josh Brunty, an associate professor of digital forensics in the School of Forensic and Criminal Justice Sciences at Marshall University to discuss the field of digital forensics, the importance of research and collaboration, and the development of dynamic academic programs. Digital forensics is still considered one of the newer forensic science disciplines. However, it is a field that is rapidly growing, with devices from smart refrigerators to video game consoles constantly collecting our data. The science behind digital forensics must be ready to pivot with every software update and additional device available on the market. Tune in as Dr. McCoy and Professor Brunty discuss digital forensics versus cybersecurity, careers and research opportunities for those with strong computer science backgrounds and an outlook for the field of digital forensics. This episode is funded by the National Institute of Justice's Forensic Technology Center of Excellence. Here's your host, Gabby DiEmma.

Gabby DiEmma [00:01:32] Hello and welcome to Just Science. I'm your host, Gabby DiEmma, with the Forensic Technology Center of Excellence, a program of the National Institute of Justice. This season, Just Science will discuss forensic science programs and NIJ funded research at universities accredited by the Forensic Science Education Programs Accreditation Commission or FEPAC. Today, we will be discussing digital forensics programs. Here to guide us in our discussion is Dr. Mark McCoy, professor and administrator of the Digital Evidence and Cybersecurity Program at the University of Central Oklahoma Forensic Science Institute. And Josh Brunty, an associate professor of digital forensics in the School of Forensic and Criminal Justice Sciences at Marshall University. Mark, Josh, welcome to the podcast. It's great to see you.

Mark McCoy [00:02:17] Thanks, Gabby.

Josh Brunty [00:02:18] Thank you, Gabby.

Gabby DiEmma [00:02:19] So Mark, tell us about your professional background and current role at the University of Central Oklahoma.

Mark McCoy [00:02:24] I spent 20 years in the Oklahoma State Bureau of Investigation as a special agent investigating a wide variety of crimes. But toward the end of my career, probably the last ten years, I was involved in the investigation and forensic examination of digital evidence and was trained to do that. I was the first supervisor of the computer crime unit in the state of Oklahoma when that unit was created, so I supervised the investigations related to computer crime and then the forensic examination of digital evidence. Yeah so that's my law enforcement career and then it led me to my academic career.

Gabby DiEmma [00:03:05] And Josh, I know you are an associate professor at Marshall University but tell me more about your professional background and current role.

Josh Brunty [00:03:12] Sure. So I started in the early 2000s as a digital forensics analyst, starting at the West Virginia State Police, working in their digital forensic unit as part of their Bureau of Criminal Investigations. I started there as an analyst, worked at different laboratories throughout the state that we had established at the time and roughly about 2006, we established a partnership with Marshall University to develop an on-campus laboratory as part of a memorandum of understanding. So that is really where my academic career starts because we were working casework at that laboratory on campus. Started teaching as an adjunct around that time of different digital forensic courses. In 2007, I was promoted to Quality Assurance Manager, which was basically creating all these SOPs for our laboratory at that time. And in 2008, I was promoted to Technical Leader of that laboratory. A position that I held until 2012 and became a professor and moved over to full-time. I have been doing that for the past 10 years.

Gabby DiEmma [00:04:27] Both of your universities have great FEPAC, accredited digital forensics programs, and I'd like to learn a little bit more about them. But for those in our audience who may not be familiar with the topic, what is digital forensics?

Mark McCoy [00:04:40] I would say a good definition would be the preservation, extraction and analyzing data found on digital devices. So that can be - range from everything from computers to the infotainment systems in vehicles and cell phones and tablets and all of those. So our field expands almost on a daily basis as more devices contain digital evidence.

Josh Brunty [00:05:07] Echoing what Mark says, you know, the landscape changes so much and so quickly. We're seeing more data move into the cloud, for example. How do we get that data out and how do we teach our individuals that are going into law enforcement or into the laboratories what to ask for in search warrants? Even little things like that. And then what do we do with these warrant returns once we get them back? How do we ingest them into our forensic tools and what does this data mean? So a big part of, I think, not just digital forensics, but forensic science in general is how do we interpret and report these results that people can understand. People on a jury, judges, prosecutors, police officers are affected by our results. And I think it's important in an accredited program that you're following this sequence of courses that teaches the students just how to do that. So, regardless of whether the student is from Marshall or Central Oklahoma, they're going to have a skill set that you know that you can rely upon and you can train and build upon. You have a good student there.

Gabby DiEmma [00:06:19] And so you both have a lot of experience with law enforcement and now with academia and you've seen this field of digital forensics kind of skyrocket in recent years just with all of the new technological advances. How do you stay on top of all of the new technologies? And how do laboratories keep up with the need for more digital forensic analysts?

Mark McCoy [00:06:43] For me in particular, I belong to some organizations, so I can keep on top of the field and still go and teach law enforcement groups about digital forensics. You know, the American Academy of Forensic Sciences is one and I belong to the International Association of Computer Investigative Specialists, which is one of the first organizations that started looking at digital forensics back in the late - in the mid-nineties.

That's the way I keep up. Other than, you know, doing the reading, research and looking at other things in the field. We do, we have to keep up on a daily basis.

Josh Brunty [00:07:18] For both of us coming out of law enforcement, I think it's important to hear what is causing the issues in the community. Where are the bottlenecks? Where are the problems? Because Apple can issue an update tonight that totally turns the ability to analyze Apple devices upside down by Monday morning, and we've seen that happen before. And those individuals that are in the agencies or in law enforcement will look back to the folks who are researching this and say, what can we do in the meantime until the tools come around to fix this? What is our path moving forward? So for me, and I know the same as for Mark, is listening and getting that feedback, and even as teaching saying, okay, well here's this method here that is changing and we're seeing this working and then start to incorporate that into the academic classrooms as well so the students can be exposed to that and they're ready for those changes when they hit the field.

Gabby DiEmma [00:08:22] In your past experience and some of the stuff we've discussed so far, I've heard the terms digital forensics and cyber, but those aren't necessarily interchangeable. So what is the difference between digital forensics and cyber?

Josh Brunty [00:08:37] Yeah, I think the easiest way, and I have to define this with students all the time and even people that you talk to in the field, we liken digital forensics to cyber and cybersecurity as DNA is to biology, where you have this very specialized area within the field of biology that has a certain task assigned to it, which is to amplify enhanced DNA and provide results from that. So in this overall landscape of cyber, you know, whether you're dealing with computer science or cybersecurity, I think digital forensics kind of fits in this little compartment that achieves those tasks. Cybersecurity is defensive, you know, countermeasures, those operations where you're trying to protect a network against an adversary and the digital forensics component of that is what happens after that whole adversary does his or her thing, what we get off of that is evidence. And I think that is where digital forensics starts, is collecting that evidence and interpreting that evidence as part of that digital forensic process.

Mark McCoy [00:09:45] Digital forensics, I would - is the collection and preservation of that data that may be used in some kind of administrative proceeding or criminal proceeding. When I think of cyber and in the way I look at cybersecurity, is more of prevention. How do we protect systems and do that? When forensics comes involved, usually something has occurred or some incident has taken place and data needs to be collected, evidence needs to be collected to figure out what happened or how it happened and who did it.

Gabby DiEmma [00:10:19] In your opinion, how does digital forensics differ from other forensic disciplines in terms of the types of technical skills needed and the educational background you really need to succeed in this field?

Mark McCoy [00:10:33] I think all forensic disciplines have some very unique skills that are needed. In digital forensics, being able to work with computers is definitely one of those skills that you need. Our academic program at the University of Central Oklahoma in our digital forensics track that's accredited through FEPAC, students have to either be a computer science major or a MIS, a management information systems major and a digital forensics major in forensic science. So when they graduate, they have a very strong computer background. That can include programing and hardware and networks and things like that, but they also have a very strong forensic background because computer scientists sometimes don't know digital forensics. It's a very different area. So - but having that strong computer background really is, I think, one of the essential skills. Now can others that maybe don't have a computer science degree? I don't, but we kind of gone through that. As long as you have some aptitude for that field, you can do well in digital forensics.

Josh Brunty [00:11:47] Yeah adding to what Mark said, I teach across two different programs here at Marshall and we have a Bachelor's of Cyber Forensics and Security. It's a whole bachelor’s program. Now, it's not the FEPAC accredited program. It's accrediting under a different body of accreditation through the NSA, but it has a different scope. It's trying to produce individuals that will go into cybersecurity jobs that may have incident response, you know, that's attached to that. You know, everyone starts at a foundation and starting to learn what the technologies are what makes a network run, what makes a computer run, what makes a cell phone run, and then building upon those technologies to, you know, talk about network protocols, for example. When you hit the send button on a text message, what happens? You know, what are the intricacies there? And that could be used for a number of different investigative means down the line. But I think, you know, on the other end of it, also teaching our forensic science program and they have a digital forensics track as part of their master's program. So they're picking up an emphasis in forensic chemistry, DNA, crime scene or digital forensics and I always tell the students, try to take on as many of those as you can because you're probably going to be working in a crime laboratory. Even if you're not interested in digital forensics, you're probably going to have a unit of digital forensics that you're going to be in charge of as a director one day. So, understanding what the requirements of those laboratories are in terms of training, equipment, expertise, facilities and understanding what their needs are. But on top of that, if they want to choose to do that, I see a lot of my old students that will go to work in a crime scene unit, and they're extracting data from DVRs and cell phones. So you never know what your job functions going to be and law enforcement is really bad about, you have expertise in this, we're going to make you do it. So I think as a student, if you're prepared to take on that responsibility to make your job easier, we certainly want to start that in the college classroom early and build that foundation for them.

Gabby DiEmma [00:14:04] So you both have kind of started talking a little bit about your programs at your universities, and I'd like to really dive into that a little bit more. So how are your programs structured? What are the students learning? How are they being prepared for this workforce?

Josh Brunty [00:14:20] So at Marshall University, forensic science focus has traditionally been around master's programs, and that was where Marshall built out of the DNA end of things and has been around for a long, long time. So as the program grew, we grew upon that program to add different areas of emphasis, and today we have four. We have DNA, forensic chemistry, crime scene and digital forensics. Now, the admission standards to get into the program sometimes will gear towards your traditional scientists and traditional science degrees. So we wanted to open up pathways where digital forensics students who might have an undergraduate degree that also want to pursue this as a full degree program in and of itself can pursue that as well. So we have different tracks. Now, our FEPAC accreditation is part of our forensic science program and we expanded that scope in 2011 to include digital forensics, which that made Marshall the first program to be FEPAC accredited in digital forensics. And that's been a growing experience because, you know, those standards have evolved over the years and so to have our curriculum. But, on top of that, they have the opportunity to either get a full-fledged master's in science, in cyber forensics and security if they choose to. They can major in forensic science with an emphasis and graduate certificate in digital forensics, or they can go get a Master of Science in cybersecurity and then pick up digital forensics as an emphasis in cybersecurity. So it really depends on what their career path is going to be and where they're incoming from. The important thing about FEPAC is that feedback looks at those core courses and examines whether or not we're teaching what's supposed to be taught in those courses. And I think there's this misconception in the - at least in the computer field, well, I don't want to box myself into curriculum. I think that is a misconception of FEPAC. We're looking at the core curriculum. There are things in this field that doesn't change every day. Networks have not changed dramatically. But it also gives a mechanism to make those changes and keep those in place. So the students, when they leave out of a program or a course, they're getting what they're supposed to be getting. So whether you step into Mark's program at Central Oklahoma or my program at Marshall, the employers know that those are - concepts are being taught regardless of the institution.

Mark McCoy [00:17:07] At the University of Central Oklahoma in the Forensic Science Institute, as I mentioned, our students can't just major in forensic science. They have to pair that with another program and they end up graduating with a dual degree. So chemistry and forensic science, biology and forensic science, criminal justice and forensic science. So - and then for digital, obviously, computer science and MIS. So our program is unique in the country to that aspect. There is no other place that requires you to basically get two degrees. But we felt it was important to have that that foundational science in a discipline. Whether it's criminal justice or chemistry or computer science, they have that good foundation to bring to, later on forensic science aspects. And in the forensic science program, if you're a digital forensic track person, you still get some very strong forensic science foundation as well. We are only one of two undergraduate digital forensics programs that are FEPAC accredited in the country, and like I said, I think we're the only one that requires those dual degrees. I think that FEPAC accreditation is beneficial for our students because it provides a set of standards that have been set by a third party, in this case, the Commission through the American Academy of Forensic Sciences and shows that a program has met those standards. So students attending those programs can be assured that they're receiving a good quality education in that field.

Gabby DiEmma [00:18:46] I'd like to take a little bit of a turn here in the conversation now and talk about research, and specifically any NIJ-funded forensic science research that you have done at your university or maybe through or with your collaborators.

Mark McCoy [00:19:03] So the Forensic Science Institute and the University of Central Oklahoma encourage undergraduate research, as well as research at the graduate level, at the master's level. We're a master's granting institution, but we have a big undergraduate research component. And some of our students, they may do an internship with a local agency, but they also can do mentored research with a faculty member as their undergraduate type capstone experience. NIJ and others have done a really nice job of helping us with equipment more than anything else. Being able to provide us the equipment that we can use then and students can use and conduct research at. The university as well has helped us out quite a bit. We've had students that would present at the national type conferences on the research they've done.

Josh Brunty [00:19:58] I know at Marshall University, at least our digital forensics and most of the forensic science disciplines would not have existed if it weren't for NIJ funding. Our partnership with the West Virginia State Police and establishing that on campus laboratory was solely funded by two NIJ-funded initiatives in 2006 and 2008, I believe. And then there was another one in 2010 to establish a teaching training partnership that's still in place to this day, long after the funds have expired. I know the NIJ funding got me to Marshall in a sense, and it helped establish that partnership and helped establish that infrastructure. Bring in the machines, you know, build the walls, you know, and get the lab established on site. And that jumpstarted that digital forensics unit that's now part of the state police's forensic laboratory now. But the nice part is that lab is still there. We can still send students to it. They can get that mentorship from analysts in that laboratory. And on top of that, you know, it helps us apply for other funds, help bring in equipment that students can put their hands on, they can get practice with. It creates infrastructure and opportunities that are just critical to advancing the field.

Gabby DiEmma [00:21:31] That's excellent. I mean, it's hard to build things from the ground up, and it's always nice to have an entity like the National Institute of Justice that kind of has your back and is helping these programs keep going and keep advancing. I'd be interested in hearing more about research at your universities. What does research look like for digital forensic scientists?

Mark McCoy [00:21:54] At UCO, we're very similar to Marshall in that we do also have a working digital forensics lab on campus. Also, the state crime lab is right across the street from the university, and that was not by accident. That was planned when the Forensic Science Institute came about and the state was looking for a new location for its crime lab. That was set up that way. So the fact that law enforcement working professionals are on campus or very near campus really fosters research. We go to the state and say, what's new? What problems are you having? What can you have us look at for you? They're work in cases. They have very little time to conduct research or do other things like that. So we get a lot of our research projects that go, then turn around and help the professionals working in the field. And digital forensics in that aspect is very applied, where it's what problem do we have now and how can we fix that? One example and this has been a few years back, but this undergraduate student presented at the American Academy of Forensic Sciences in the digital multimedia section, you know, remember when the Xbox 360 came out? I mean, that's a few years back, but it came out with the Kinect. I remember sitting there and my son who was younger at the time, we have a Kinect and he plays a game and right after there's pictures of him playing the game and spent 20 years in law enforcement, I said, oh, that's I didn't say, oh, that's neat, I said, I wonder where those pictures are on that Xbox. The Xbox 360 has a very unique file system. It doesn't - it's not anything that's common. So I went to Dr. Adams and said, I'd like to buy some Xboxes, and which is, you know, that's a - that's not a request you get normally, but in digital forensics it is. And we bought some Xboxes and the undergraduate student conducted some experiments starting from scratch and imaging the Xboxes and then playing the game and then imaging again and looking for those images and where they were stored and she was able to locate them. So she presented to local law enforcement who at the time were seeing Xbox 360s in their lab and were able to help them determine where those images might be. And then just this year, we had a student present at the American Academy on the flaw with Zoom and the ability to transmit a URL to the user, attendee in Zoom without their knowledge and a page opening up. So kind of interesting that we get to do some kind of unique research and so there's always opportunities, new devices, new opportunities for digital forensics research.

Josh Brunty [00:24:50] And like UCO, you know, we have the state crime lab is in close proximity to campus. Not just DNA, but the digital forensics lab as well. So you see these unique devices come in that they have no idea how to process and we started to see smartwatches come in and wearable devices and IoT devices and got, you know, an inordinate amount of requests at the state level. Can you process these? So a few years prior, right before the pandemic, we used some of the contract money that we had and funded a student to look at that problem to see if we can get data extractions from wearable devices and IoT devices. She was very successful in doing so and that methodology has ported over to some of the commercial tools that you see now. But she presented that at the American Academy of Forensic Sciences. And so, you know, these students, they take on these projects that are maybe small one scale, and they're borne out of these, you know, universities around the country and then they start to trickle up to these other laboratories, other universities build upon them. You see collaborative projects that will spring up, that will get, you know, presented at the Academy meeting. So you never know what you're going to see. I'm waiting on someone to drag a smart fridge into the state's lab and say, you know, we know there's data on this. Can you get it off? But I know that some of the things that we're looking at now just on the horizon is IoT devices like Amazon Echoes, you know, where we're still constantly evolving how do we get data off of that? Not just in the cloud, but at the device level. Smartwatches are changing and evolving too. Apple watches, Android watches. We see more and more doorbell camera requests. You know, do those doorbell cameras hold anything on premises or in the cloud? And then there's this whole enigma of the dark web. You know what? What do we do when data is out there? And cryptocurrency? You know, how do we trace this back? So there's so many problems that are just hitting at once, you know, that students can almost pick an area that's of interest and if they approach that the right way, they'll have a good project that will help law enforcement. Because those are the problems that they're facing right now. I know if I were back on the bench in the lab, those would be the things that would stop me, because there's no there's nothing out there to help right now. So even if I have a watch and - on the desk in my lab, can they figure out a way and replicate a way for me to get data from there? And that was where the Academy presentation came in that we had really good success with and we published on that in the Journal of Forensic Sciences.

Gabby DiEmma [00:27:43] In terms of the students who do engage in this research, do you find that they're more likely to pursue graduate studies? Or do they find that it's easier to get jobs? And it sounds like they're extremely involved in the different professional organizations. So I'd like to hear about the impact that this research has on the future careers of these students.

Mark McCoy [00:28:08] I think student's opportunity just to conduct research is important because Josh and I both working in a crime lab at the time when we had a question, we had to be able to say, I wonder how this data got here, and I'm going to have to explain it somewhere, maybe in court so I need to conduct an experiment to determine how it got there. So even working in that they have to be able to design and conduct some experiments while on the job. So that training to do research while they're an undergraduate or graduate student is vital because they're going to continue to do that through their whole career. They're going to troubleshoot things, they're going to ask questions and then have to design things to find out what the answer is. And usually that answer is important because it's going to be scrutinized in some public forum, most likely in court. They’re so many new questions on a daily basis, and I think just that inquiring mind, so to speak, is attractive to employers. Knowing that there's always something to learn, that you have to be, you know, a lifelong learner in this profession.

Josh Brunty [00:29:24] Adding to what Mark says, I think it's important for students and I fully agree with him, and students have to learn how to ask the right questions to conduct this research because it's so important to their career. And these are things they're going to be doing in the laboratory. So, you know, when they start these, even these small research projects, where do they go to ask these questions? What sources do they use? You know, it's not always just a simple Google search. It's going out and asking people in the community. What can I do? What's out there? And knowing where to go to find those sources? That's something that not only helps them as a student, but it also shows them this is a source I can go back to as an employee one day. And I know Mark has to deal with this a lot, but I have a lot of students that will contact me back and say, I've got this case in my lab. Far, you know, 10 years removed as a student and asked for opinions and say, can you help me get to this point? And in many cases, those are where some of these student projects are born out of. Well, I don't know how to fix this, but I have a student here that's willing and able to pick that up as a summer research project. That is really important for students early on to start to get involved in these organizations, to start to network. Not just with people in the community but interfaced with people at other universities and at an Academy of Forensic Sciences meeting, you'll see these university students get together and they're talking about their research and they're talking with other employers because they're going to be working in the field with each other one day. And that's what you want to see. You want to see that interaction happen while they're students because they're going to be such a good ambassador and representative of your university when they leave and go back and mentor students in the future. That's an important aspect of this as well, is that mentorship process.

Gabby DiEmma [00:31:26] I'd be curious to hear more about the types of careers that this type of education, this type of pathway. What else have they been up to?

Mark McCoy [00:31:35] Many of them do go into law enforcement at the federal, state, local level as computer forensic examiners, but many of them go to the private sector as well. So I think the opportunities are kind of wide reaching.

Josh Brunty [00:31:51] Yeah, I know when I started teaching, not just when I was working in the laboratory, but when I started teaching, most of our students were going into law enforcement. They were going to crime laboratories and digital forensic laboratories. I'm seeing a shift now where companies and these organizations are hiring and not just the companies, but retail organizations that have their own digital forensics and incident response. If you can think of a Fortune 500 company, they have a digital forensics person and they have an incident response person. They have, you know, security operations centers, which are hybrids where, you know, kind of sits in the middle between digital forensics and cybersecurity. So there's fun little niche jobs out there that a student that's coming in that may think, well, okay, I'm going to go to work in a crime laboratory. They're leaving and working at a retail organization, or they go from a crime lab or a digital forensics lab to one of those organizations, as you know, and get a very hefty pay bump because of it. So I think the field is very - it's growing in that aspect because companies, every company needs these people now because they're trying to protect their assets both internally and externally, but they're trying to recreate these events that happen. So I think it's important as we - I know at Marshall, how do we grow and let students realize that those careers exist while still teaching in this FEPAC accredited program?

Mark McCoy [00:33:27] As Josh was talking, I just remembered that one of the largest digital forensics labs is with Walmart. Walmart has a huge digital forensics presence in that company. So students that maybe don't want to pursue a law enforcement career, there are plenty of other opportunities in this field.

Gabby DiEmma [00:33:45] Excellent. Yeah, it sounds like a really booming industry. A lot of different pathways you can take from this sort of education. Before we wrap up, are there any final thoughts you would like to share with our listeners?

Mark McCoy [00:33:57] I just would encourage anybody that has an interest in forensic science and digital forensics in particular to look at the possibilities or, you know, find Josh and I on the website and send us an email. We'd be happy to answer any questions. I know I would or give us a call and anything we can do to mentor students in that area. I know I would like to do so.

Josh Brunty [00:34:21] It's important to talk about, at least to me, of how important digital forensics is going to be over the next 10 years, 20 years, 30 years. There's a big need for this. And I encourage any students, the same as Mark, you know, get in contact with us, you know, don't hesitate. If you have the slightest interest in this, pursue it. It's a very, very fruitful, wonderful opportunity. So if the interest is there, get in contact with us. Even if it's just about research, you may not even want to be a student at the university, but you are listening to this and you have a skill set and I want to reach out and help. We need help in the field, you know, whether it's, you know, research or whatever the case, we certainly want to build this field because this is a people issue and we want to help people with what we're doing. That's the most important thing about this is helping people. And that's what I want to convey to students, convey to the field that everything we do is about helping people and solve the people problem.

Gabby DiEmma [00:35:29] And thank you so much for agreeing to be on our podcast. I mean, it's been a pleasure talking to you both today and I'm just so glad that we were able to have this platform to talk about digital forensics more.

Mark McCoy [00:35:42] Thank you.

Josh Brunty [00:35:43] Thank you.

Gabby DiEmma [00:35:43] So if you are a listener at home or on your drive and you enjoyed today's episode, be sure to like and follow Just Science on your platform of choice. And for more information on today's topic and resources in the forensics field, visit ForensicCOE.org. I'm Gabby DiEmma, and this has been another episode of Just Science.

Voiceover [00:36:08] Next week, Justin sits down with Dr. Christine Picard from Indiana University, Purdue University, Indianapolis, and Jessica Zarate from Madonna University to discuss impression and pattern analysis FEPAC programs. Opinions or points of views expressed in this podcast represent a consensus of the authors and do not necessarily represent the official position or policies of its funding.