FORENSIC FOCUS
FOR DIGITAL FORENSICS AND EDISCOVERY PROFESSIONALS

http://www.forensicfocus.com/c/aid=100/interviews/2015/arnim-eijkhoudt-researcher-amp-lecturer-university-of-applied-sciences/
Interviews - 2015
Arnim Eijkhoudt, Researcher & Lecturer, University of Applied Sciences

Posted Sunday March 29, 2015 (14:58:38) (1296 Reads)


Arnim Eijkhoudt

Arnim, we caught up with you last year about Uforia. Could you tell us a bit about what's been happening with the project since then?

Well, what we had in Amsterdam was more of a proof of concept really, to show what we could do with big data visualisation in the case of forensic investigations and ediscovery. Over the past year or so – I think it's about a year now – we've developed it into something that is close to being actually usable, in the sense that you could use it in production. So it's more or less stable, it works, you can put in random data.

As a challenge, to see if it works ourselves, we put together a cell phone example where you could put in tower logs that providers send you and timeline that and it worked as expected, so we've grown much more confident that it all actually now is becoming something resilient which you can use in an investigation.

What are you planning on developing over the next few months? Are there any additional elements we'll be seeing?

Mostly what we're looking towards now is actually integrating a few key parts, such as reporting features and ways of grabbing and tagging the data, which is important if you're doing the reporting part. You can tag the data that you're interested in, and either export it or tag it with keywords or a summary of why you're tagging it, and then automatically generate reports for it. That will be one of the key features.

Otherwise, mostly what we'll be focused on is adding functionality for specific usage scenarios. A lot of the attendees and people I showed this to asked if it can do network forensics, in the sense of can I give it a log or a pcap file, or something like that. And I tell them yes every time, but it still needs the module to do that. It's not really a problem to program the module, but it's purely a question of time, and the quick way we had to put certain things together for the conference.

You mentioned that talking to people at DFRWS has led you to look at various aspects that could be more fine-tuned. How has Uforia changed to take into account feedback from different areas of the digital forensic world?

In a way, even when I look back at what we started when we were doing Uforia, we were primarily initially looking at things from a digital investigation point of view, from a forensic expert. But the student that's currently working with me at University, said it would be easy to make this much more generic. So even though it initially started as a project where the primary goal was forensic investigations, it kind of morphed into a product where you can throw any kind of data in and it's turning much more into a generic visualisation framework as well.

So we never thought about security experts at first, but they have all been asking: "Can we give it pcap or Netflow data?", "Can we use this to see if there's an unusual spike in a certain amount of traffic and find out what is happening?". Uforia seems to cover a need by many experts to give broad overviews of big data using generic visualisation, but without losing that detailed view of the data I mentioned – you always see these network graphs and they normally follow these nice regular wave-like patterns. If there's suddenly a huge spike or dip, that's going to trigger the attention of people. So almost by accident we're starting also to cover other use-cases.

Then we started thinking: why not implement searching for any kind of documents (documents in the legal sense)? There was an important court case in Ireland recently where experts had to go through 680,000 documents. It was a landmark case, because the Court ruled that Technology Assisted Review (TAR) complied with the rules governing [legal] discovery. And we were thinking, rather than having to go through documents manually or only by document type, we could offer even more efficient searches with Uforia. We realised that with some minor changes, we could group documents (this time in the 'productivity sense': Word, Excel, E-mail, etc.) together and offer type-agnostic searches. Eoghan Casey also touched on this with his comments at the DFRWS about the classification of data; we already tried to build this in: you can group any kind of evidence items together. So regardless of whether you're speaking about emails, documents, Excel sheets: there is always an 'author', and you can now have a unified search for that field. So Uforia has really spun off in a different direction from how I initially envisioned it. But rather than narrowing

its use down to a specific use-case or group of users, it gradually became a generalised exploration and visualisation tool instead.

Have you picked up on anything from DFRWS specifically that you think would be useful to develop further over the next few months?

Standardisation of all aspects of forensic investigations is really a challenge we hadn't considered or thought of yet. I don't really think we have a standard for visualisation, to give you an example. This was also mentioned by Eoghan, but standardisation in description, visualisation, etc. will be very useful: regardless of whether you're in a court setting or talking to fellow experts, if you can quickly show that your product is standardised and everyone speaks the same unambiguous 'language', that will be a great improvement.

We've been talking a lot this week about trying to get law enforcement, academia and corporate to all work together. How important do you think that is, and how do you think we can make it happen?

Well, I chaired the discussion group during the conference, and what struck me is that everyone is pretty much in agreement that the disconnect in communication between the different expertises is a problem, and we think that we were all quickly in agreement that visualisation and standardisation are very good ways of getting everyone on the same page. You know the famous saying: “a picture says more than a thousand words.” On the one hand, it can hide incomprehensible technical details from a legal expert or a law enforcement officer, but by the same token it's just as useful within a corporate setting to make information easily visible and understandable for management. For instance, I frequently talk to people who work in auditing or CERT/CSIRT teams: they need these tools just as much, because they have to report to and convince their management in no uncertain terms about what they have discovered. There have already been significant gains in visualising information, but most of the older tools tend to be geared towards expert users, often after extensive training. So that's where we think the future should be, in one word: empowerment.

You lecture as well, and we have a lot of students on the boards who are coming to the end of their studies, and want to know how to make themselves stand out. Do you have any advice for them?

I think it's mostly this: the great students I've seen over the years are the ones who are passionate and able to turn that passion into knowledge and deeds. You really don't have to be brilliant at every subject!

In his keynote on Tuesday, Troels Oerting was talking about the need to work with the social sciences. Do you think that's important even for companies who are developing

tools rather than conducting investigations?

I think it's crucial actually. It's as much about how you convey the message as how you construct it. I'm a man of taglines and management buzzwords, apparently! But you're absolutely right: even from the design perspective, you can have the nicest-looking design, but if it has lots of little niggles constantly, hinders the way you have to collaborate, or uses difficult, ambiguous, contextual or cultural wording because there's not been any communication standard: that's an absolute killer. So collaborating with the social sciences is actually very important, because they can give this extra perspective about user experience, interaction and communication that might not always come from working with the development teams.

What sort of backgrounds do your students come from?

From my experience, we get all sorts of students. IT obviously might be a notorious field and joked about for having socially awkward students, but we've done (and we still do) a lot of international projects over the years, and our international projects are always interdisciplinary and multicultural.

For example, we've done international projects in ediscovery over the years with partners from many different cultures and expertises: we worked with a French university, Croatian university, English university, with students coming from all over the world, and often from very different disciplines. There were students from Sweden who were into digital archiving and archiving-related studies, legal students from the Netherlands, we had students who were hardcore programmers, database engineers, so a mix of very different fields.

How easy was it for the students to learn to collaborate across disciplines, and what do you think they gained from the experience?

Well in the span of barely two weeks they got amazing results: partly because of their passion, partly because of their intrinsic motivation (they signed up), but for a considerable part it was also due to their diversity. The project setting forced them to cooperate and to quickly learn how to understand each other and talk to each other, because they came from all these interdisciplinary fields and cultures. I can tell you that it can cause a lot of drama and can be hard to sort out in such a short time, but at the end the students had really fantastic results in their investigations. Many of the students made life-long friendships during these projects!

As an example, when the IT students were talking to the legal students, they realised that the implications of some of the things they were proposing were questionable at best. So I really think that the discussions that we had during DFRWS with regard to not just standardising the tooling, but also standardising the format we exchange and do things in,

makes absolute sense. I don't mean it just in the technical sense of how we talk to each other, but a unified, objective language in a way. There's a lot we could gain there.

Is there anything else you'd like to add?

The only thing I would add is: please collaborate with us! This is a very diverse field, and compared to last year's DFRWS I believe attendance has doubled. Personally I think it's a shame that there aren't more people from the US, Asia and the Middle East. I'm here with a colleague who is on sabbatical from Cape Town University in South Africa. With existing transatlantic partnerships and agreements worldwide, it's going to be more and more crucial that we all continue to talk to each other, and I think DFRWS should take the lead and try to set the gold standard for many of the subjects we talked about.

Arnim Eijkhoudt is a lecturer in e-discovery, digital forensics and IT security at the University of Applied Sciences in Amsterdam. He also works on Uforia, a universal investigation and visualisation tool. You can find out more at www.uforia.nl.

Forensic Focus interviewed Arnim at DFRWS, the annual Digital Forensics Research Workshop, which took place in Dublin from the 23rd-26th of March. Next year's workshop will be held in Lausanne, Switzerland, from the 29th March - 3rd April. You can find out more and register here.