FORENSIC FOCUS
FOR DIGITAL FORENSICS AND EDISCOVERY PROFESSIONALS

http://www.forensicfocus.com/c/aid=86/interviews/2014/arnim-eijkhoudt-lecturer-in-digital-forensics-university-of-applied-sciences/
Interviews - 2014

Arnim Eijkhoudt, Lecturer in Digital Forensics, University of Applied Sciences

Posted Tuesday August 05, 2014 (18:34:56) (2360 Reads)

Arnim Eijkhoudt

Arnim, please tell us about your role as a lecturer in digital forensics, and how you first became interested in the field.

I've been fascinated with 'tinkering' with computers from a young age: figuring out why things (don't) work, reverse-engineering, reconstructing what happened and so on. Therefore, it was natural for me to turn to the fields of Forensics and Security after I studied Informatics and became a lecturer. Before 2007 I was already incorporating Computer Security-related topics into my lectures and classes where possible. From 2007 to 2013, the Amsterdam University of Applied Sciences and the University of Amsterdam have offered a joint Minor in Forensic Intelligence & Security (MINFIS).

Together with a colleague from the UvA I set up a comprehensive programme that combined our knowledge of both fields. I took over as head of the minor in 2012 and since then we have managed to make it even more successful: we consistently have more signups than we can accept, with students from all over the Netherlands contacting me to see if they can participate.

My primary role as lecturer is twofold: I am one of the key lecturers for the Forensics and Security courses and projects, and I take care of the overall logistics, planning, arranging for guest lectures, etc.

You're currently working on Uforia, a universal forensic indexer and analyser, which was showcased at DFRWS earlier this year. Tell us more about the project and the challenges it aims to address.

A friend and I came up with the idea of Uforia as a back-end for a search engine or for simple file deduplication. After building a simple test version, we realized it could be expanded to do much more. I set out to redesign Uforia as a modular, scalable and flexible framework for parsing the metadata of all files on a filesystem, based on the detection of their MIME-types. I developed a working, complete proof-of concept in 2012. From 2012 onwards, the research and development on Uforia was continued through the EDiscovery lectorate group (http://ediscoverynl.dmci.hva.nl/), part of Create-IT Applied Research (http://www.create-it.hva.nl/). As one of the lectorate members, I am actively directing and supervising the continued development of Uforia as a student project in the minor programme. Most of the back-end code has since been rewritten, and in late 2013 we started developing the website as the first 'front-end' for exploring the stored information.

Uforia is designed to store discovered information in a simple, compatible yet descriptive way, so that the ways of using the data remain as flexible as possible. Because of this design, we can employ powerful search technology and visualization tools like ElasticSearch and d3js to give insight into the data *and* deduce internal relationships.

Uforia has already changed significantly since the last time we saw it in May; what can we expect from it in the future? Are there any new developments planned for the next year or so?

As of this writing, we should be finishing our first version of the Documents search and Admin panel. There are still many plans for Uforia, but for the next year or so we hope to finish:

- recoding the main engine in C/C++ for speed
- a comprehensive admin interface
- exploring the possibilities of visualizing pcap-/Netflow-dumps
- tagging evidence items for automated evidence report generation
- reworking the search results to allow for quick subselections.

Anyone who is interested in Uforia's progress or who wants to experiment with its features is welcome to visit our 'live demo' website at http://www.uforia.nl.

You teach forensic intelligence & security at the Hogeschool van Amsterdam. What common challenges do you see your students having to overcome during their forensics education, and what would you say makes a successful student in this area?

The most commonly recurring challenge for students has always been to overcome their (understandable) focus on 'catching the bad guy' in their courses and projects, wanting to explain to everything rather than applying critical thinking every step of the way.

One of the ways we teach our students to overcome this, is by incorporating legal & ethics subjects into our courses/lectures. The most successful students are those that quickly pick up on these subjects and begin to apply critical thinking to everything they write and do.

Finally, what do you do to relax when you're not working?

I enjoy traveling, particularly by motorcycle, and spending time with my family.

Arnim Eijkhoudt is a lecturer and digital forensics professional at the University of Amsterdam, where he teaches Forensics, Security and System & Network Engineering. The Uforia project is a simple, flexible and extensible framework for forensic analysis and parsing of file metadata.