1000 - Secret Tools: Learning about Government Surveillance Software You Can't Ever See

Friday at 10:00 in Track 4
20 minutes | 0025
Peyton "Foofus" Engel*Attorney at Hurley, Burish & Stanton, S.C.*

Imagine that you're accused of a crime, and the basis of the accusation is a log entry generated by a piece of custom software. You might have some questions: does the software work? how accurate is it? how did it get the results that it did? Unfortunately, the software isn't available to the public. And you can't get access to the source code or even a working instance of the software. All you get are assurances that the software is in use by investigators around the globe, and doesn't do anything that law enforcement isn't supposed to be doing. Because you can trust the government, right?

This talk will look at a family of tools designed for investigating peer-to- peer networks. By synthesizing information from dozens of search warrant affidavits, and a few technical sources, we're able to put together at least a partial picture of the software's capabilities. But we'll also look at the reasons the government offers for keeping these tools out of the public eye and talk about whether they make sense. Finally, we'll examine the implications that investigations based on secret capabilities have for justice.
Peyton "Foofus" Engel
After 18 years in IT, with 16 of those years spent in security and penetration testing, Foofus now works as an attorney. But because he's got significant experience with the Internet and security, one area of his practice focuses on consulting with litigants where digital evidence is at stake. In this capacity he does forensic analysis and assists other attorneys with strategy for presenting (or calling into question) computer-based evidence. In his spare time, Foofus enjoys cooking, playing guitar, and opera. Oh, and remember CoffeeWars? Foofus was pretty involved with that

#defcon25/by_track/track4/Friday
#defcon25/By_Day/_Friday