

# 1000 - I Know What You Are by the Smell of Your Wifi

Sunday at 10:00 in Track 2

20 minutes | Art of Defense, Demo, Tool, Audience Participation,

**Denton Gentry\*Software Engineer\***

Existing fingerprinting mechanisms to identify client devices on a network tend to be coarse in their identification. For example they can tell it is an iPhone of some kind, or that it is a Samsung Android device of some model. They might look at DHCP information to know its OS, see if the client responds to SSDP, or check DNS-SD TXT responses.

By examining Wi-Fi Management frames we can identify the device much more specifically. We can tell a iPhone 5S from an iPhone 5, a Samsung Galaxy S8 from an S7, an LG G5 from a G4. This talk describes how the signature mechanism works.

Specifically identifying the client is the first step toward further scanning or analysis of that client's behavior on the network.

Denton Gentry

Denton Gentry is a software engineer who has worked at a lot of places and plans to work at a few more.

[#defcon25/by\\_track/track2/Sunday](#)

[#defcon25/By\\_Day/\\_Sunday](#)