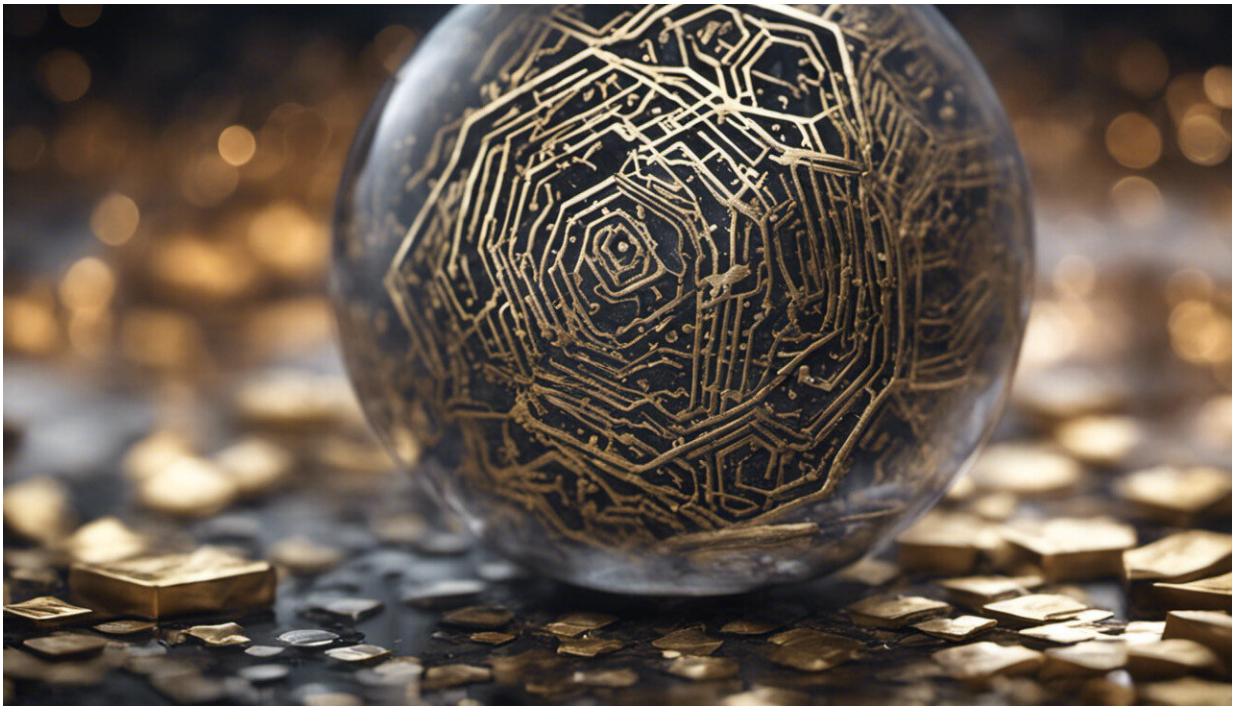
Wi-Fi devices goldmine for investigators

January 6 2016, by Rob Payne, Sciencenetwork Wa



Credit: AI-generated image (disclaimer)

Timely access to Wi-Fi devices at crime scenes could provide police with vital evidence, including placing suspects at the location.

This is due to their ability to record information from mobile devices, including successful or failed attempts to log into a network, de-authentication times and MAC addresses.

A MAC address is a unique identifier that provides information such as mobile device make and model and even what you've named it.

Edith Cowan University PhD candidate and WA Police technical advisor Dan Blackman suggests Wi-Fi devices could be equally or more valuable than GPS.

"These devices could hold a lot of information, but we're not capturing it," Mr Blackman says.

"If we were to look at it from a purely legal perspective, we might be able to place a specific person at a specific location at a specific time, which is gold in terms of evidence for a court setting."

Surely, it can't be that easy..

A number of challenges need to be overcome, including how little time investigators might have to act.

"A lot of these devices and personal routers have a limited amount of information and memory," Mr Blackman says.

A series of tests revealed that older devices had as little as 204 kilobytes of storage, which filled in seven and a half minutes and led to overwriting of memory.

Even newer devices were limited, filling within eight minutes when faced with sustained authentication attempts.

And turning the unit off simply exacerbates the problem.

"If we power off the Wi-Fi device we lose a heck of a lot of data, which causes issues with seizure," Mr Blackman says.

This limitation makes getting the device to a police lab difficult, while the size of WA makes sending an investigator to the scene equally problematic.

The solution may involve modifying a faraday bag—enclosed carrier units that block connectivity to cellular networks, Wi-Fi and Bluetooth—to accommodate power cords or USB power strips.

Contamination is another issue, as several of the examined devices had both external and internal antennae.

"So the moment you disconnect the external aerial, [the internal] fires up, and you still have connectivity to the device," Mr Blackman says.

This could lead to unexpected and unwanted network traffic from forensic investigators and scene guards.

However, Mr Blackman says the ever-increasing reach of Wi-Fi, especially in public areas, makes the technology a potential game-changer.

This article first appeared on ScienceNetwork Western Australia *a science news website based at Scitech.*

Provided by Science Network WA