Street View cars record nearby WiFi access-points. The purpose of this is to provide an alternate to GPS. A computer without GPS can scan for nearby access-points, look up their location in Googles database, and figure out its own location. This is similar to the service provided by the company Skyhook Wireless, or by the collaborative effort WIGLE.
Google Map captures the signal strength in the decode. Google can use this to triangulate the location of the device that sent the packet. Street View knows the precise GPS location of the car as it rolls down the street.

If it can get three beacons (or other data packets) from the access-point, it can triangulate the position of the access-point. Moreover, if it stores the raw packets from one day as the car takes one route, it can correlate the packets with another days packets on a different route.

Even though the access-point MAC address is cached, theres extra data in the packet. These extra data will include URLs, fragments of data returned from websites (like images), the occasional password, cookies, fragments of e-mails, and so on.

Google sniffed packets, only caring about MAC addresses and SSIDs, but when somebody did an audit, they found that the captured packets occasionally contained more data, such as URLs and e-mail fragments.

(DNR - to me, it exposes a wifi security flaw for wardrivers)

Read the full story there:

https://erratasec.blogspot.com/2010/05/technical-details-of-street-view-wifi.html