***What is a browser fingerprint?/How do you create a browser fingerprint?***

*You can collect info about the “browser” such as font lists of the computer, dimensions of the screen, a plugins list, the OS, and so on. By extracting this information through various techniques such as going fullscreen, and making script requests, you can make a “fingerprint” of that browser, which can be used to identify you.*

***How reliable is browser fingerprinting as a tool to track individual users?***

*This varies by implementation. For example, many browsers are very difficult to fingerprint as they do not have a lot of information to distinguish between them through mobile browsers and browsers with javascript disabled.  
But on the other hand, the vast majority of people will not be disabling their javascript as that would likely stop the main functionalities of many websites. You wouldn’t be able to access popular sites like facebook, sites wouldn’t be able to load videos, and so on.  
Overall, it is very dependent on how you choose to view it. Although in the near future, more of these potential tracking features may be found.*

***How do you connect a fingerprint to its previous fingerprints when they change?***

*Browser fingerprints would likely change in small increments. Identifying aspects such as plugins or installed fonts are not very likely to change often, so when someone has a new fingerprint, you can identify them by looking at those first, and then seeing how different their old fingerprint is to their possible new fingerprint. Features of the fingerprint such as websites they’re logged or their IP may be more dynamic, so those should be lower on the priority list when comparing fingerprints.*