**Question 1**

root@kali:~# iwconfig

[checks for wireless connection]

root@kali:~# airmon-ng start wlan0

[place card into monitor mode]

root@kali:~# airodump-ng mon0

[begin capturing traffic]

root@kali:~# airbase-ng -a [target client BSSID] --essid "Starbucks" -c [any number but 2] mon0

[create access point with client SSID, MAC and ESSID - channel number must be different to the original AP value]

root@kali:~# aireplay-ng --deauth 0 -a [target client BSSID]

[deauthenticate client off their original AP]

root@kali:~# iwconfig wlan0 txpower [max region power]

[adjust power signal to 'hide' original AP]

**Question 2**

* As the DHCP server issues an IP address to the client, this could be compared against the original target address.
* Password acceptance (if you intentionally input a false password and it's accepted, then it's probably the fake AP).
* Checking for non-standard IP addresses - relies on previous knowledge of the network.
* An 'unsecure' label may be attached to the counterfeit network which might indicate it.
* Use a wireless intrusion prevention system (WIPS) that scans the network for unauthorised setups - mainly institutionally based.
* Overwhelming signal strength (that may be unusual in context of the cafe's usual service).
* Device notifications may alert of connection transfers, which may indicate the presence of the fake network.
* A majority of prevention protocols lie with the end-point protection and detection schemes situated within the network space.
* Ping the router's MAC address (on the router) and compare against an ARP table - however it doesn't account for MAC aliases/clones.

Generally, it's hard to distinguish a legitimate service from a malicious service if it has been setup well. The best advice would be to refrain from connection, use a VPN or get the owner to reset/turn-off the router to determine the legitimate source and then act accordingly.

**Question 3**

Fluxion is a relatively new attack and is around 3-4 years old. It uses both technical and social aspects to phish individuals. By analysing the WPA handshake, the original network is then jammed and replaced with a cloned replica that entices users to restart and re-authenticate their credentials. This allows the technology to intercept and gather network security information which can be escalated from here on. However, this is a relatively basic attack which can easily be detected by AP systems and is also dependent on the quality of the source used. Hence this attack should only be focused on weak and obscure networks - mainly afflicting personal/home networks and public Wi-Fi access points due to the lack of security and overall potential to phish individuals. Using this tactic on a smaller scale (smaller target of individuals) can be extremely effective and easy to accomplish as it requires next to no technical knowledge. This also helps to avoid detection on a smaller scale, which would probably be the ideal scenario based on the type of attack to be conducted.

**Question 4**

DNS spoofing occurs when DNS records are maliciously altered to redirect traffic to a target site (often also malicious). Often, these destination sites are cloned replicas, which entice clients to input sensitive information which is then garnered by the attacker for further use. First, cache poisoning is injected into servers which can be housed for different periods of time (depending on the TTL). Once this server is compromised, it acts as a MiTM attack that funnels traffic away from the intended destination. This can be combined with an evil twin attack as the evil-twin launches a hotspot which can then redirect traffic to a set server (or hacker - MiTM) which can bypass the need to spoof DNS servers with malicious addresses (as the hacker can inject data at the point of the connection to the hotspot rather than at the server).