Q1: Why are the “Finished” messages in SSL/TLS important?

Q2: Why or how might a user visit a bad website like attacker.com?

Q3: Consider a website site.com that includes a third-party script, e.g.:
   <script src="http://otherdomain.com/library.js"></script>
   If this script sets a cookie, under what origin will that cookie be set?
   From what origin can this script read cookies?