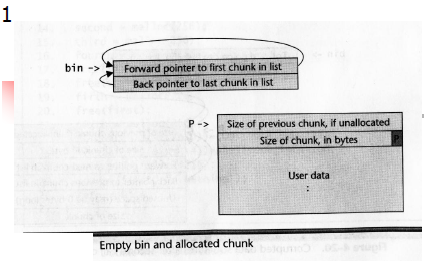
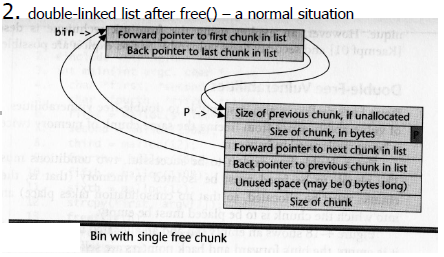
Опасностите при двойно освобождаванена паметта се появява при опит блок памет да бъде освободен 2 пъти без да бъде локализиран между освобождаванията.

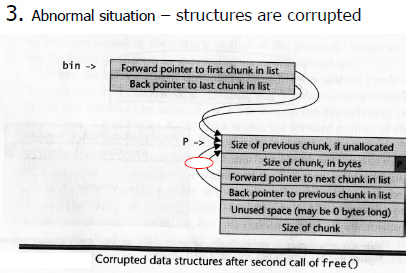
За да се злоупотреби с двойното освобождаване на паметта трябва да бъдат изпълнени 2 условия:

\*Блока с памет трябва да е изолиран в паметта

\*Мястото кадето ще бъде поставен блока трябва да бъде празно







Ако се появи заявка за памет в този момент, локатора на памет ще се опита да локализира блок от бин-а и ще успее. Unlink() макрото ще се задейства за да се извади блока от бина, без да променя пойнтерите. Ако се появи още една заявка за памет със същата големина като резултат ще се върне същия блок, което е грешка. В тази ситуация може да се използва malloc() с цел изпълняването на недоброжелателен код.

Пример:

