Количество пакетов, необходимое для атаки

1 вопрос:

Выбранный ответ: 1 пакет.

Вообще в ходе выполнения домашнего задания я использовала два последовательных пакета (потому что так показалось проще и занимало меньше времени), однако в этом нет необходимости, для нахождения разделяемого секрета (если заведомо известно, что процесс аутентификации пройден успешно) достаточно и одного пакета типа Request, берем из него значения всех полей и используем написанный в первом задании алгоритм.

2 вопрос:

Выбранный ответ: два последовательных пакета, идущие в разные стороны (первый - от RADIUS к NAS, второй - от NAS к RADIUS).

Здесь уже точно нужно два пакета, причем последовательных, причем первый должен идти от RADIUS-сервера. Сначала берем значение EAP-MD5 Value из request-пакета (в коде я его обозначаю md5ChallengeValue), а также значение из responce-пакета (оно обозначено md5ResponceValue), тут одним пакетом мы уже не обойдемся. Конкатенируя ID, пароль и md5ChallengeValue и взяв от этой конкатенации хеш, мы и получим md5ResponceValue. Итог: нам надо два пакета, ну а то как они идут (сначала от RADIUS к NAS, второй: от NAS к RADIUS) - это уже определяется тем, какие именно пакеты мы смотрим: request и responce, где есть необходимый Md5-Challenge-EAP