Let \((Gen, H)\) be a collision-resistant hash function and let \(F\) be a PRF. For each of the following, state whether \(\hat{H}\) is necessarily collision resistant. Justify your answer.

1. \(\hat{H}^s(x_1||x_2) = H^s(x_1 \oplus F_s(x_2))\) No.
   
   **Attack:** Choose arbitrary \(x_1, x_2, x'_2\)

   Set \(x'_1 = x_1 \oplus F_s(x_2) \oplus F_s(x'_2)\) [note adv can find such \(x'_1\) since \(s\) is public]

   Output \(x_1||x_2, x'_1||x'_2\)

   \[
   \hat{H}^s(x_1||x_2) = H^s(x_1 \oplus F_s(x_2)) \\
   \hat{H}^s(x'_1||x'_2) = H^s(x'_1 \oplus F_s(x'_2)) = H^s(x_1 \oplus F_s(x_2) \oplus F_s(x'_2) \oplus F_s(x'_2)) \\
   = H^s(x_1 \oplus F_s(x_2)).
   \]

2. \(\hat{H}^s(x_1||x_2) = H^s(H^s(x_1)||x_2)\) Yes.

   Assume towards contradiction that an attacker finds \(x_1||x_2 \neq x'_1||x'_2\) such that \(\hat{H}^s(x_1||x_2) = \hat{H}^s(x'_1||x'_2)\).

   Then \(H^s(H^s(x_1)||x_2) = H^s(H^s(x'_1)||x'_2) = y\)

   Let \(y_2 = H^s(x_1)||x_2\)

   \(y'_2 = H^s(x'_1)||x'_2\)

   **Case 1:** \(y'_2 \neq y_2\). Then we have found a collision on the outer instantiation of \(H^s\) since \(H^s(y_2) = H^s(y'_2) = y\).

   **Case 2:** \(y_2 = y'_2\). Then \(x_2 = x'_2\). Since \(x_1||x_2 \neq x'_1||x'_2\), it means that \(x_1 \neq x'_1\). But this means we have found a collision on the inner instantiation of \(H^s\) since \(H^s(x_1) = H^s(x'_1)\) in order for \(y_2 = y'_2\).