- Question:

How do I decrypt the encrypted IKE v2 packets on Landslide IPSec test cases (e.g. IP Application Node with IPSec V2, Site to Site Nodal).

- Answer:

When trying to decrypt the encrypted IKE v2 packet, in wireshark trace, edit preferences and select ISAKMP.

From there, you need to fill out the following:

Initiator SPI (this is the Initiator Cookie)

Responder SPI (this is the Responder Cookie)

SKEY_ID_ai (this is the generated authentication key for the initiator side)

SKEY_ID_ar (this is the generated authentication key for the responder side)

SKEY_ID_ei (this is the generated encryption key for the initiator side)

SKEY_ID_er (this is the generated encryption key for the responder side)

For the SKEY information we'll need to look at a trace level 10, since these keys are generated.

For SKEY_ID_ai - search the log using this string: "SKEYID_a value"

For SKEY_ID_ar - search the log using this string: "SKEYID_ar value"

For SKEY_ID_ei - search the log using this string: "SKEYID_e value"

For SKEY_ID_er - search the log using this string: "SKEYID_er value"

For example, in ts.log.9:

2070| Fri Aug 12 19:01:33.711175| ../src/ipsecTunnelInitiatorIkeSharedKeyState.cc| 408| handleModExpEvent| Debug| SKEYID_a value: d8 c3 64 f5 de b5 72 fe 1d 08 44 b3 23 9c 30 45

2070| Fri Aug 12 19:01:33.711180| ../src/ipsecTunnelInitiatorIkeSharedKeyState.cc| 412| handleModExpEvent| Debug| SKEYID_ar value: 21 2c 8b d3 10 f9 fa f5 c4 fb ad b4 32 c7 01 1e

2070| Fri Aug 12 19:01:33.711185| ../src/ipsecTunnelInitiatorIkeSharedKeyState.cc| 416| handleModExpEvent| Debug| SKEYID_e value: 10 1a de 36 32 b1 ba 35 87 53 b1 55 d7 3b 10 82

2070| Fri Aug 12 19:01:33.711190| ../src/ipsecTunnelInitiatorIkeSharedKeyState.cc| 420| handleModExpEvent| Debug| SKEYID_er value: 8d d6 d3 26 f0 51 7f 6e b9 6c 02 cc 66 e5 b5 69

The value of SKEYID as below, so you are able to decrypt the IPSec packets via these values.

SKEYID_a value: d8c364f5deb572fe1d0844b3239c3045

SKEYID_ar value: 212c8bd310f9faf5c4fbadb432c7011e

SKEYID_e value: 101ade3632b1ba358753b155d73b1082

SKEYID_er value: 8dd6d326f0517f6eb96c02cc66e5b569