EECS 4482 Assignment 2

1. AH Transport – Capture 2.

The most likely mode of operation for Capture 2 is AH Transport because in the ICMP message the next header points to ICMP, which would indicate that the packet is **not** encapsulating the entire datagram, but only the payload of the datagram. This indicates that it is in AH Transport mode.

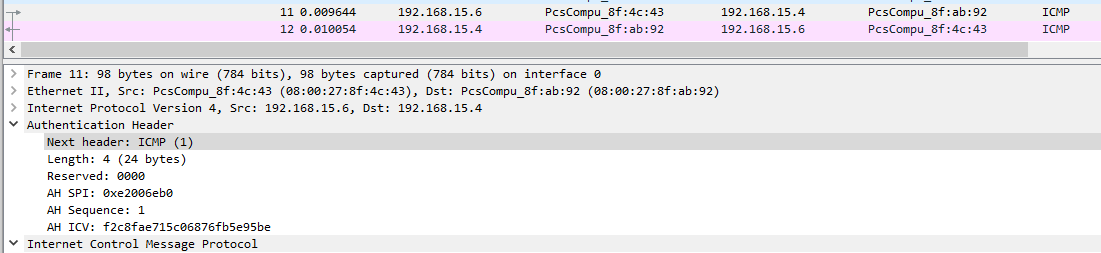


Figure 1 ICMP packet of Capture 2. Next header is ICMP.

AH Tunnel – Capture 4.

The most likely mode of operation for Capture 4 is AH Tunnel because in the ICMP message the next header points to IPIP, which would indicate that the packet is encapsulating the entire IP datagram. The packet size is also larger than in capture 2 due to the extra IP headers. This indicates that it is in AH Tunnel mode.

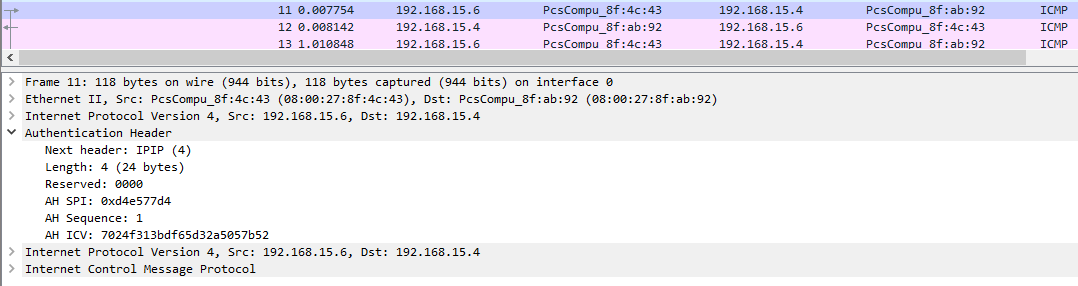


Figure 2 ICMP packet of Capture 2. Next header is IPIP.

ESP Transport – Capture 3.

The most likely mode of operation for Capture 3 is ESP Transport because it contains ESP packets and the size of the packets are 84 bytes. This is smaller than the 100 byte ESP size in Capture 1 because it is only encapsulating the payload and not the whole datagram. This indicates that it is in ESP Transport mode.



Figure 3 ESP packet of Capture 3. The size is 84 bytes.

ESP Tunnel – Capture 1.

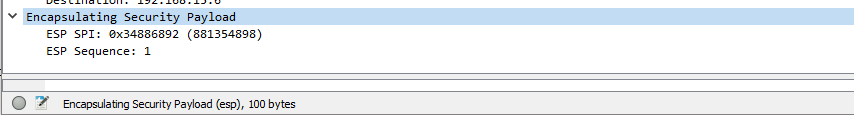
The most likely mode of operation for Capture 1 is ESP Tunnel because it contains ESP packets and the size of the packets are 100 bytes. This is larger than the 84 byte ESP size found in Capture 3 suggesting that these packets encapsulate the payload and the IP header. Therefore the IP header seen is another IP header assigned so the packet can be transported. This indicates that it is in ESP Tunnel mode. 

Figure 4 ESP packet of Capture 1. The size is 100 bytes.

1. 1) The variant of Diffie-Helman algorithm that Host 1 offers Host 2 is DH2: Alternate 1024-bit MODP group, which is found in both proposals that host 1 offers in the first ISKAMP packet (figure 5) under IKE Attribute stating Group-Description in the Security Association Payload (1). Since there is only 1 DH algorithm offered, in the second ISAKMP packet they agree on using the previously stated algorithm (figure 6). This is the same for all captures.

2) Host 1 offers 2 symmetric-encryption algorithms in the first ISAKMP packet. These symmetric-encryption algorithms are AES-CBC and 3DES-CBC (figure 5). In the second ISAKMP packet Host 2 accepts the first proposal containing the AES-CBC symmetric-encryption algorithm (figure 6). It is also important to note that the hash algorithm they are using is also found here and it is SHA. This is the same for all captures.

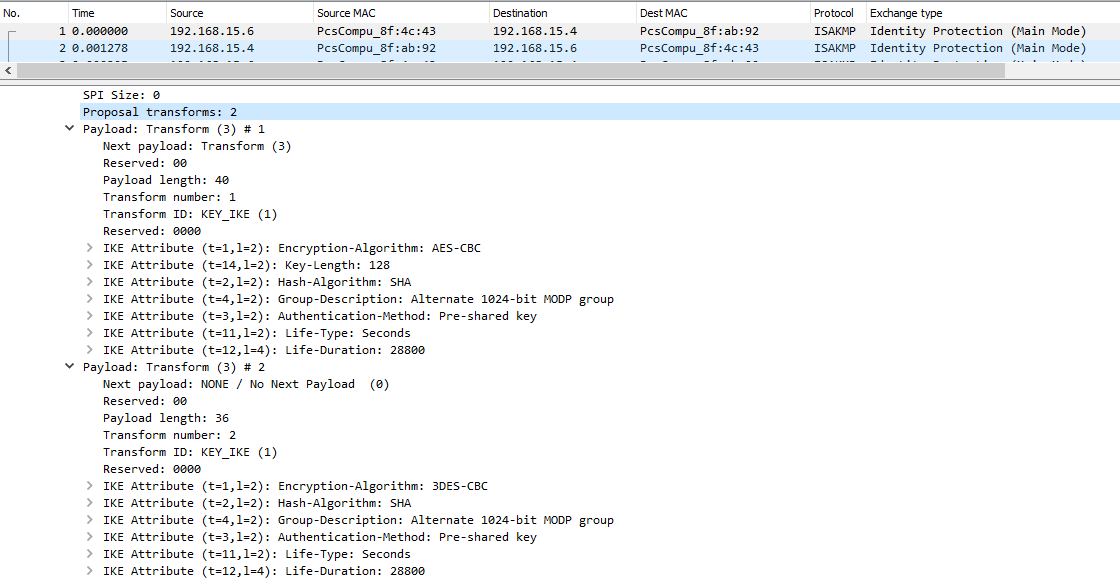


Figure 5 ISKAMP packet 1 of Capture 1. This shows the 2 proposals, which state the variant of the Diffie-Hellman algorithm (question 1) and the symmetric-encryption algorithms (question 2) offered in the first ISKAMP packet. This also shows the authentication method used (question 4). This is the same for all captures.

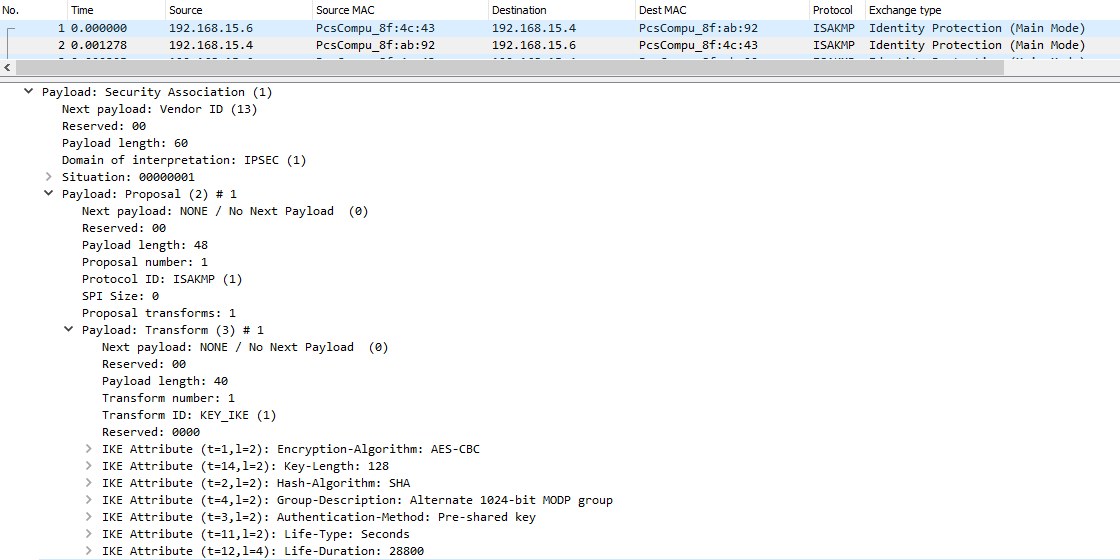


Figure 6 ISKAMP packet 2 of Capture 1. This shows the variant of the Diffie-Hellman algorithm (question 1) and symmetric-encryption algorithm (question 2) proposal chosen in the second ISKAMP packet. This also shows the authentication method used (question 4). This is the same for all captures.

3) Host 1 and Host 2 start exchanging encrypted content from the 5th packet (figure 7). This is after they have determined the Diffie-Hellman algorithm, Symmetric-encryption algorithm and hash algorithm and have exchanged their nonces. This is the same for all captures.

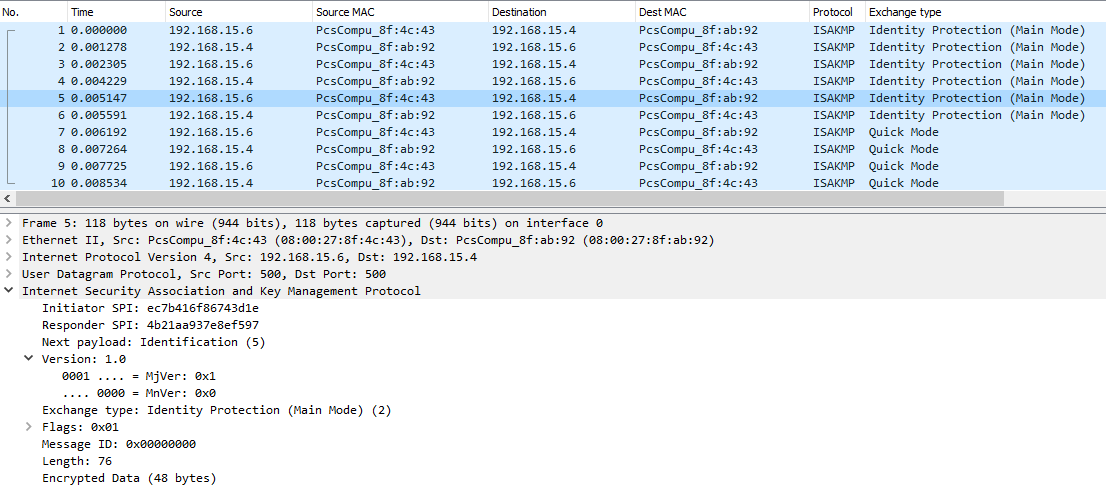


Figure 7 After the 4th ISAKMP packet, the data is encrypted. This the same for all captures.

4) The authentication method used between Host 1 and Host 2 is pre-shared key (figure 5 and figure 6). This means that they are using a pre-shared secret key and was determined by looking at the authentication method provided in the first and second ISAKMP packets in the Wireshark captures.

1. 1) The fields that are the same for both IP headers are the version number, header length, flags, source IP address and destination IP address (figure 8). The fields that are different for both IP headers are the total length (105 vs 60) , ID (0x4ebe vs 0x4ebd), protocol (AH vs ICMP) and header checksum (figure 9).

2) Yes because this allows authentication over the whole datagram and not just the payload. This means that the end user will know that the packet is coming from the right host (i.e. not a spoofed IP address). Even if the packet can be read by others, the packet will not likely be spoofed or have values that have changed mid transmission. If it has then the end user will know because the hash key won’t match upon arrival.

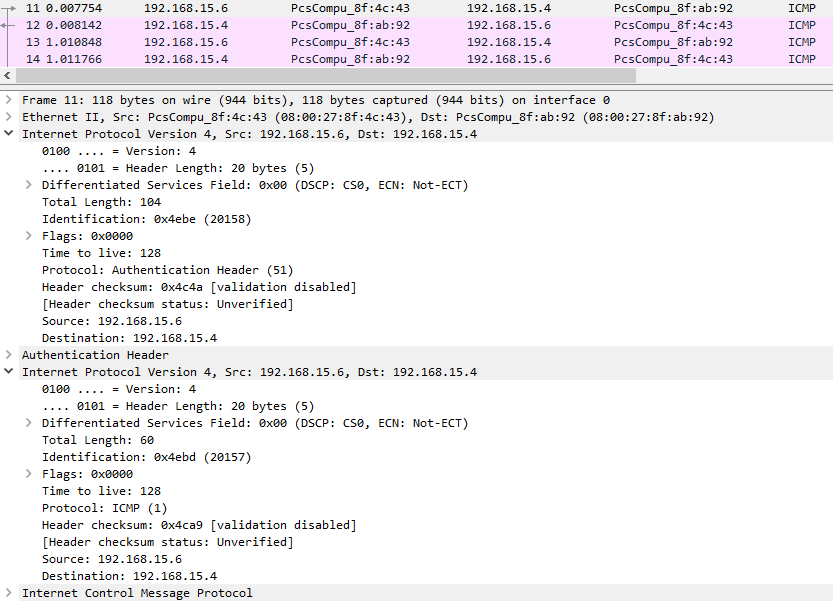


Figure 8 This ICMP packet shows the similarities between the original and newly added IP headers.

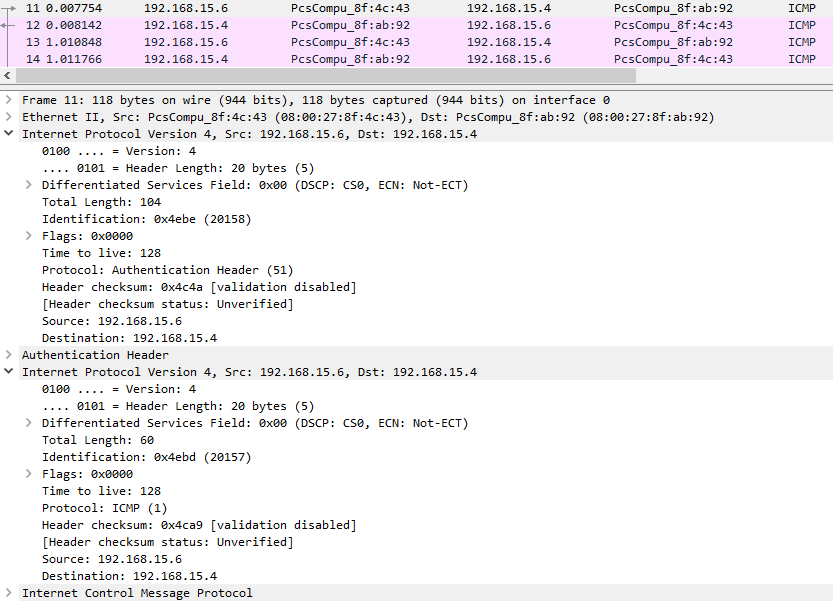


Figure 9 This ICMP packet shows the differences between the original and newly added IP headers.

1. The DH half key for host 1 is: 80b41e697cc87a9fb90749ee371e9ad71289ac411a6833bd021d0de90471d432511ee305553f4c903110297bd17c7a836df91b1c4554fcef50da409b850dcc99686dfadcea724896cd485dacb33ceb90d2dbcfcdc4a22b3f1e237d56b4ba00d79eb0f2284befccb40f5aa19f54190f39ab84bc2f6ab6e4f0b7fa8aa489955460.

The DH half key for host 2 is:

57f5d57135c2cd4a6a2eef6f7ad5a936e4f922bb97d06b13e5157c3733ef08d572ce9f0fb708885376061b76b2ebf7bb955819d0b52e14f5636549fa3086aadd40e0062bf823e50d62b880a7752a66d168481a28a52da473fde53468e3713c7daa769170314ece89708ffb4299f366453b09e39f441c7d47a01e686126380fd7.

These are 128 byte keys are found in the third and fourth ISAKMP packets respectively under the Key Exchange (4) payload (figure 10 and figure 11).

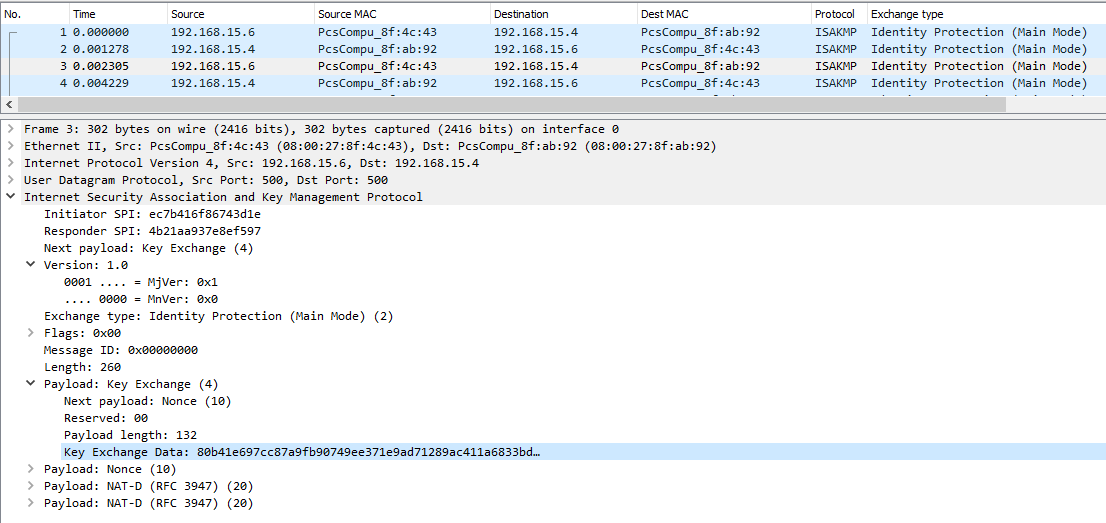


Figure 10 The third ISAKMP packet displaying the DH half key for Host 1.

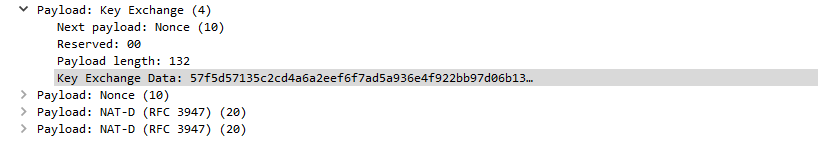


Figure 11The fourth ISAKMP packet displaying the DH half key for Host 2.