4.10 Experiment No. 10

Aim:

To study the IPsec (ESP and AH) protocol by capturing the packets using Wireshark tool.

.

Theory:

The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

What Ports Does IPSEC Operate On?

UDP port 500 should be opened as should IP protocols 50 and 51. UDP port 500 should be opened to allow for ISAKMP to be forwarded through the firewall while protocols 50 and 51 allow ESP and AH traffic to be forwarded respectively.2

What is ISAKMP?

ISAKMP stands for Internet Security Association and Key Management Protocol. These are two key components of an IPSEC VPN that must be in place in order for it to function normally and protect the public traffic that is being forwarded between the client and VPN server or VPN server to VPN server.

What are ESP and AH?

No, ESP is not Extra-Sensory Perception! ESP stands for Encapsulating Security Protocol and AH stands for Authentication Header.

Encapsulating Security Protocol

ESP gives protection to upper layer new protocols, with a Signed area indicating where a protected data packet has been signed for integrity, and an Encrypted area which indicates the information that's protected with confidentiality. Unless a data packet is being tunneled, ESP protects only the IP data payload (hence the name), and not the IP header.

ESP may be used to ensure confidentiality, the authentication of data origins, connectionless integrity, some degree of traffic-level confidentiality, and an anti-replay service (a form of partial sequence integrity which guards against the use of commands or credentials which have been captured through password sniffing or similar attacks).3

Authentication Header

Authentication Header (AH) is a new protocol and part of the Internet Protocol Security (IPsec) protocol suite, which authenticates the origin of IP packets (datagrams) and guarantees the integrity of the data. The AH confirms the originating source of a packet and ensures that its contents (both the header and payload) have not been changed since transmission.

If security associations have been established, AH can be optionally configured to defend against replay attacks using the sliding window technique.4

How Do They All Work Together?

When properly configured, an IPSEC VPN provides multiple layers of security that ensure the security mode and integrity of the data that is being transmitted through the encrypted tunnel. This way an organization can feel confident that the data has not beenintercepted and altered in transit and that they can rely on what they are seeing.

IPsec Protocols

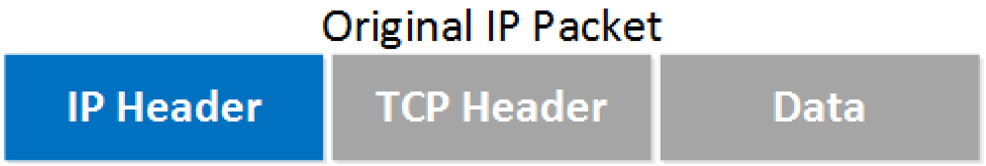
AH and/or ESP are the two protocols that we use to actually protect user data. Both of them can be used in transport or tunnel mode, let's walk through all the possible options.

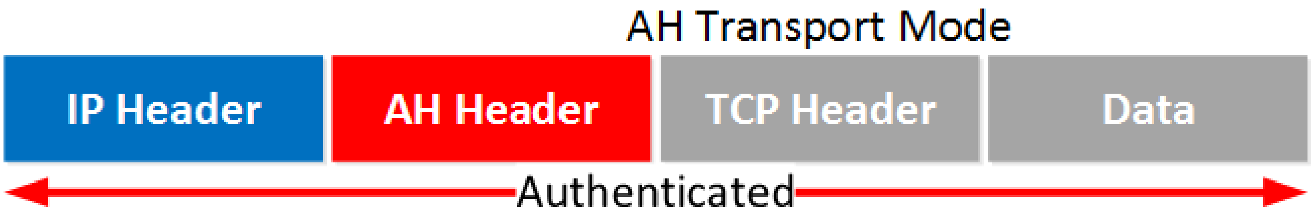
Authentication Header Protocol

AH offers authentication and integrity but it doesn't offer any encryption. It protects the IP packet by calculating a hash value over almost all fields in the IP header. The fields it excludes are the ones that can be changed in transit (TTL and header checksum). Let's start with transport mode…

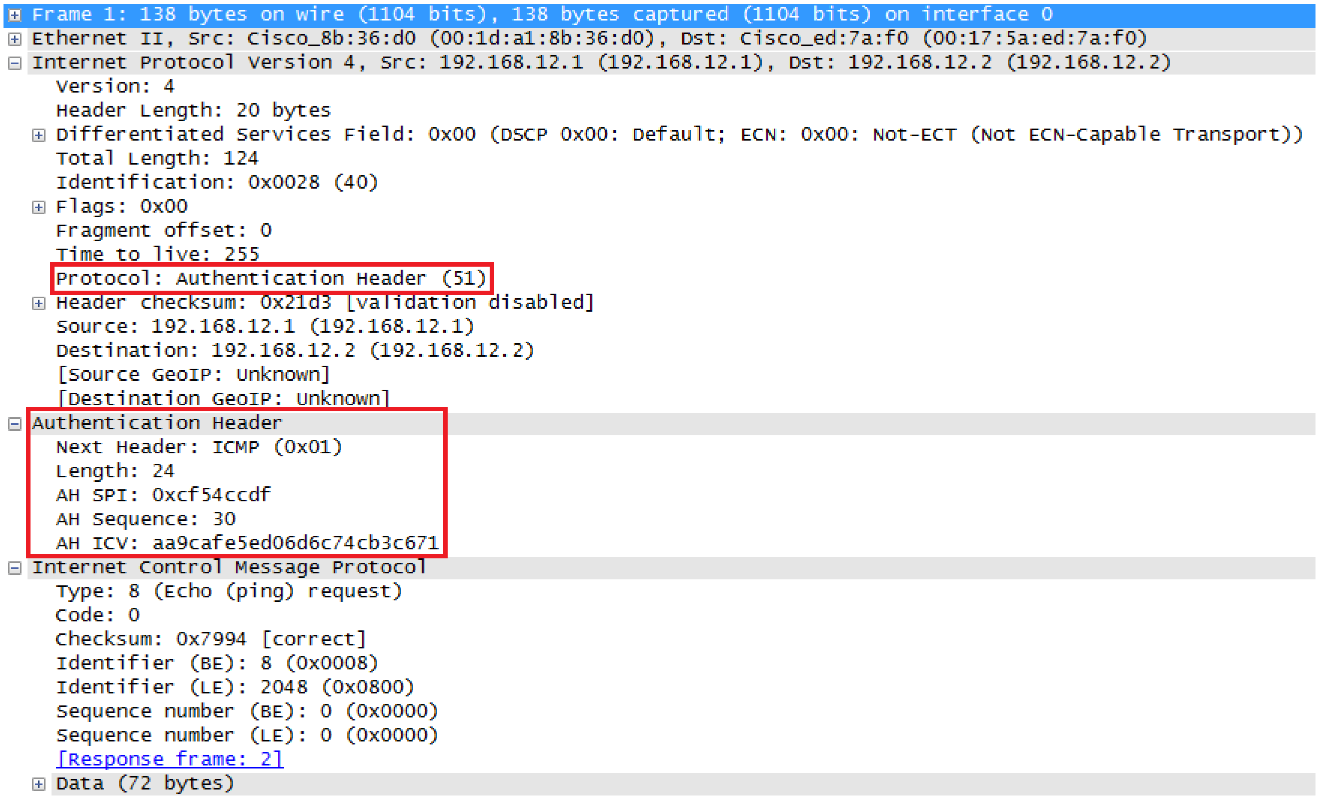
Transport Mode

Transport mode is simple, it just adds an AH header after the IP header. Here’s an example of an IP packet that carries some TCP traffic:





And here’s what that looks like in Wireshark:



```
⊞ Frame 1: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
⊞ Ethernet II, Src: Cisco_8b:36:d0 (00:1d:a1:8b:36:d0), Dst: Cisco_ed:7a:f0 (00:17:5a:ed:7a:f0)
⊟ Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 124
    Identification: 0x0028 (40)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: Authentication Header (51)
  ⊞ Header checksum: 0x21d3 [validation disabled]
    Source: 192.168.12.1 (192.168.12.1)
    Destination: 192.168.12.2 (192.168.12.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Authentication Header
    Next Header: ICMP (0x01)
    Length: 24
    AH SPI: 0xcf54ccdf
    AH Sequence: 30
    AH ICV: aa9cafe5ed06d6c74cb3c671
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x7994 [correct]
    Identifier (BE): 8 (0x0008)
    Identifier (LE): 2048 (0x0800)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Response frame: 2]
  ⊞ Data (72 bytes)
```

Above you can see the AH header in between the IP header and ICMP header. This is acapture I took of a ping between two routers. You can see that AH uses 5 fields:

Next Header: this identifies the next protocol, ICMP in our example.

Length: this is the length of the AH header.

SPI (Security Parameters Index): this is an 32-bit identifier so the receiver knows towhich flow this packet belongs.

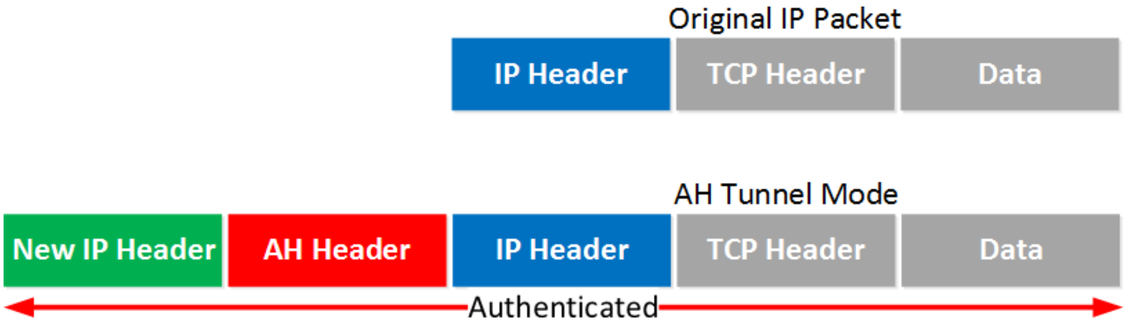
Sequence: this is the sequence number that helps against replay attacks.

ICV (Integrity Check Value): this is the calculated hash for the entire packet. The receiver also calculates a hash, when it’s not the same you know something is wrong.

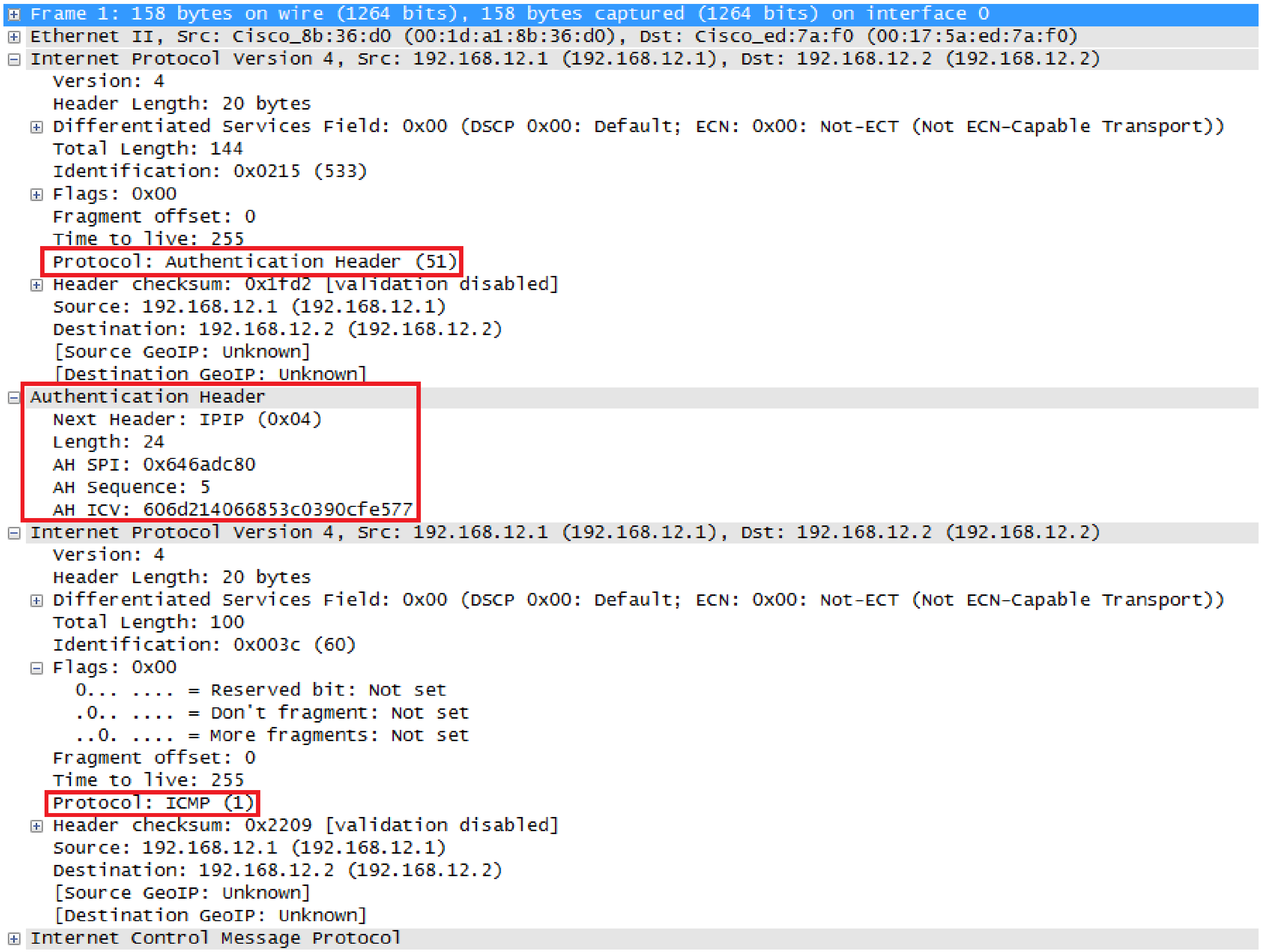
Let’s continue with tunnel mode.

Tunnel Mode

With tunnel mode we add a new IP header on top of the original IP packet. This could be useful when you are using private IP addresses and you need to tunnel your traffic over the Internet. It’s possible with AH but it doesn’t offer encryption:



The entire IP packet will be authenticated. Here’s what it looks like in wireshark:



```
⊞ Frame 1: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface 0
⊞ Ethernet II, Src: Cisco_8b:36:d0 (00:1d:a1:8b:36:d0), Dst: Cisco_ed:7a:f0 (00:17:5a:ed:7a:f0)
⊟ Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 144
    Identification: 0x0215 (533)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: Authentication Header (51)
  ⊞ Header checksum: 0x1fd2 [validation disabled]
    Source: 192.168.12.1 (192.168.12.1)
    Destination: 192.168.12.2 (192.168.12.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Authentication Header
    Next Header: IPIP (0x04)
    Length: 24
    AH SPI: 0x646adc80
    AH Sequence: 5
    AH ICV: 606d214066853c0390cfe577
⊟ Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 100
    Identification: 0x003c (60)
  ⊟ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x2209 [validation disabled]
    Source: 192.168.12.1 (192.168.12.1)
    Destination: 192.168.12.2 (192.168.12.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ Internet Control Message Protocol
```

Above you can see the new IP header, then the AH header and finally the original IP packet that carries some ICMP traffic.

One problem with AH is that it doesn’t play well with NAT / PAT. Fields in the IP header like TTL and the checksum are excluded by AH because it knows these will change. The IP

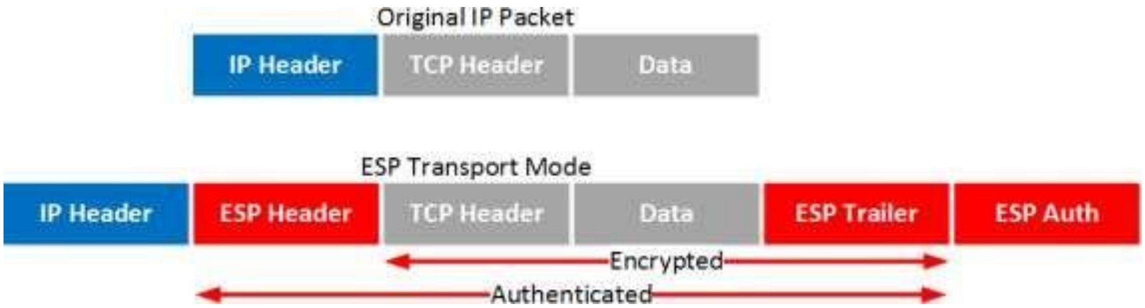
Let’s continue with ESP…

ESP (Encapsulating Security Payload) Protocol

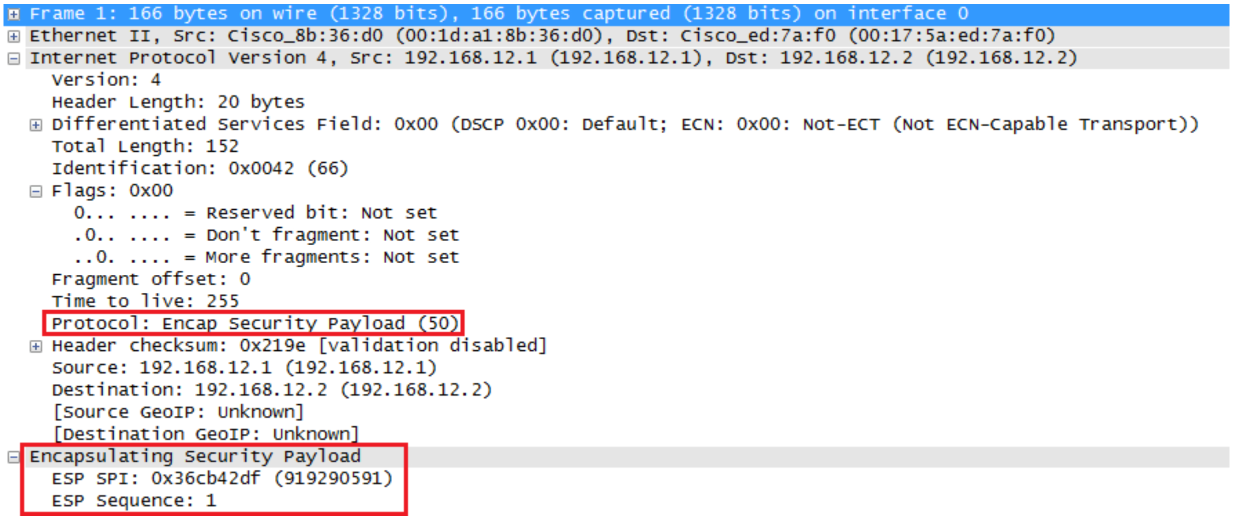
ESP is the more popular choice of the two since it allows you to encrypt IP traffic. Wecan use it in transport or tunnel mode, let’s look at both.

Transport Mode

When we use transport mode, we use the original IP header and insert an ESP header. Here’s what it looks like:



Above you can see that we add an ESP header and trailer. Our transport layer (TCP for example) and payload will be encrypted. It also offers authentication but unlike AH, it’s not for the entire IP packet. Here’s what it looks like in wireshark:

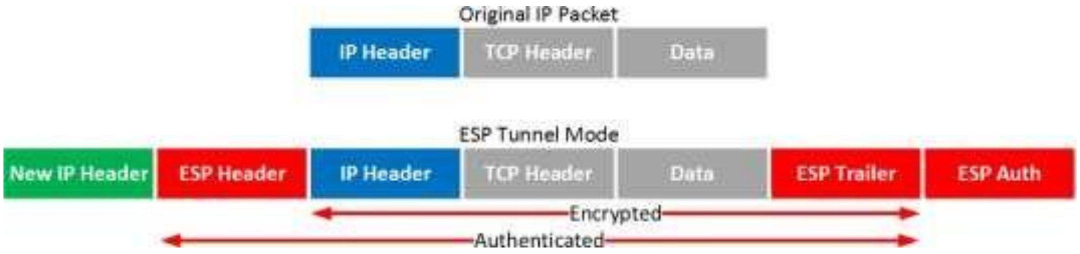


```
⊞ Frame 1: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0
⊞ Ethernet II, Src: Cisco_8b:36:d0 (00:1d:a1:8b:36:d0), Dst: Cisco_ed:7a:f0 (00:17:5a:ed:7a:f0)
⊟ Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 152
    Identification: 0x0042 (66)
  ⊟ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: Encap Security Payload (50)
  ⊞ Header checksum: 0x219e [validation disabled]
    Source: 192.168.12.1 (192.168.12.1)
    Destination: 192.168.12.2 (192.168.12.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Encapsulating Security Payload
    ESP SPI: 0x36cb42df (919290591)
    ESP Sequence: 1
```

Above you can see the original IP packet and that we are using ESP. The IP header is incleartext but everything else is encrypted.

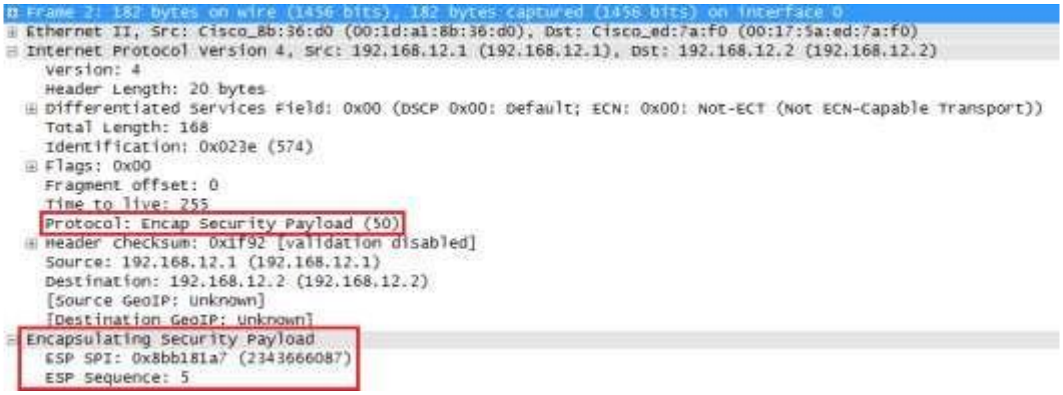
Tunnel Mode

How about ESP in tunnel mode? This is where we use a new IP header which is usefulfor site-to-site VPNs:



It’s similar to transport mode but we add a new header. The original IP header is now also encrypted.

Here’s what it looks like in wireshark:



```
⊞ Frame 2: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface 0
⊞ Ethernet II, Src: Cisco_8b:36:d0 (00:1d:a1:8b:36:d0), Dst: Cisco_ed:7a:f0 (00:17:5a:ed:7a:f0)
⊟ Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 168
    Identification: 0x023e (574)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: Encap Security Payload (50)
  ⊞ Header checksum: 0x1f92 [validation disabled]
    Source: 192.168.12.1 (192.168.12.1)
    Destination: 192.168.12.2 (192.168.12.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Encapsulating Security Payload
    ESP SPI: 0x8bb181a7 (2343666087)
    ESP Sequence: 5
```

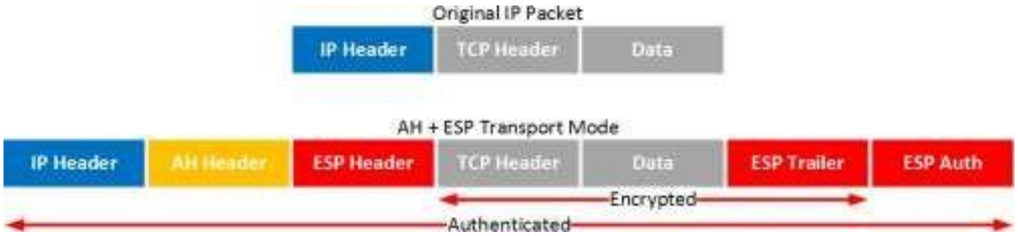
The output of the capture is above is similar to what you have seen in transport mode. The only difference is that this is a new IP header, you don’t get to see the original IP header.

AH and ESP

This one confuses a lot of people, it’s possible to use AH and ESP at the same time. Let’s check it out!

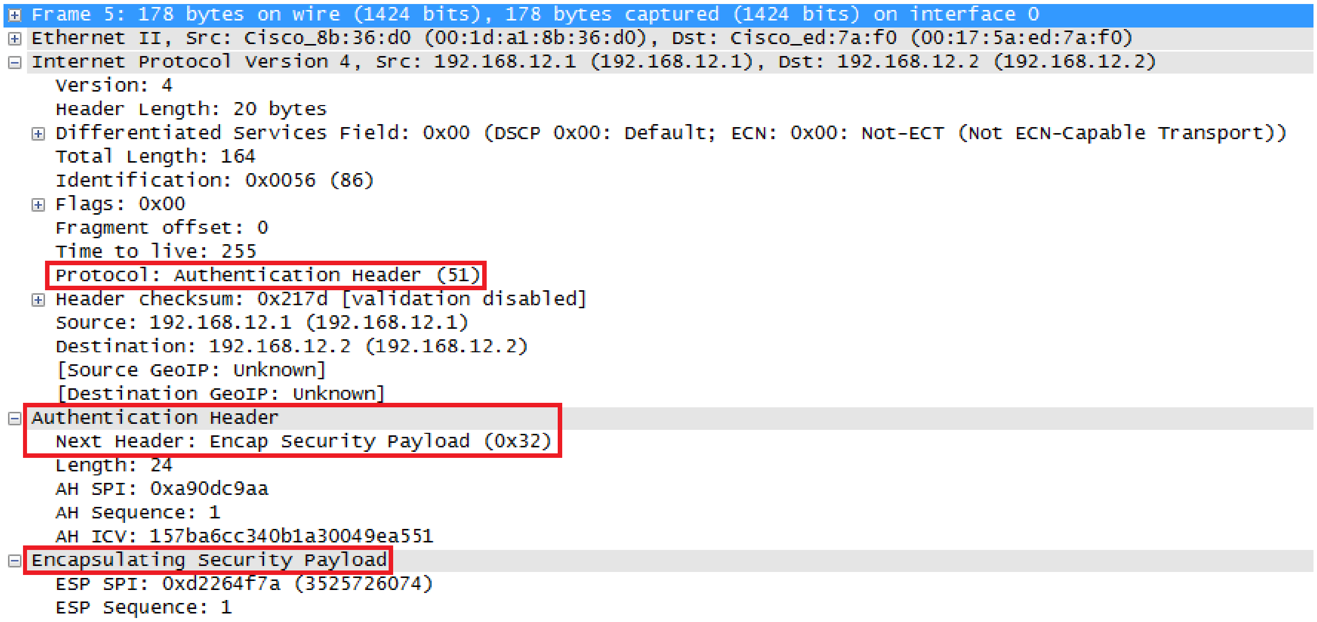
Transport Mode

Let’s start with transport mode, here’s what the IP packet will look like:



With transport mode we will use the original IP header, followed by an AH and ESP header. The transport layer, payload and ESP trailer will be encrypted.

Because we also use AH, the entire IP packet is authenticated. Here’s what it looks likein wireshark:



```
⊞ Frame 5: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface 0
⊞ Ethernet II, Src: Cisco_8b:36:d0 (00:1d:a1:8b:36:d0), Dst: Cisco_ed:7a:f0 (00:17:5a:ed:7a:f0)
⊟ Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 164
    Identification: 0x0056 (86)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: Authentication Header (51)
  ⊞ Header checksum: 0x217d [validation disabled]
    Source: 192.168.12.1 (192.168.12.1)
    Destination: 192.168.12.2 (192.168.12.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Authentication Header
    Next Header: Encap Security Payload (0x32)
    Length: 24
    AH SPI: 0xa90dc9aa
    AH Sequence: 1
    AH ICV: 157ba6cc340b1a30049ea551
⊟ Encapsulating Security Payload
    ESP SPI: 0xd2264f7a (3525726074)
    ESP Sequence: 1
```

Above you can see the original IP packet, the AH header and the ESP header.

Conclusion:

Hence we had studied the IPsec (ESP and AH) protocol by capturing the packets using Wireshark tool.

Outcomes:

Retrieve IPsec (ESP and AH) protocol by capturing the packets using Wireshark tool.

FAQs:

1) What is Wireshark?
2) Why Wireshark is used?
3) How the Packets are Captured in Wireshark?