COMPUTER NETWORKS AND SECURITY LABORATORY

Group C
Assignment No. 17

NAME :- OJUS P. JAISWAL

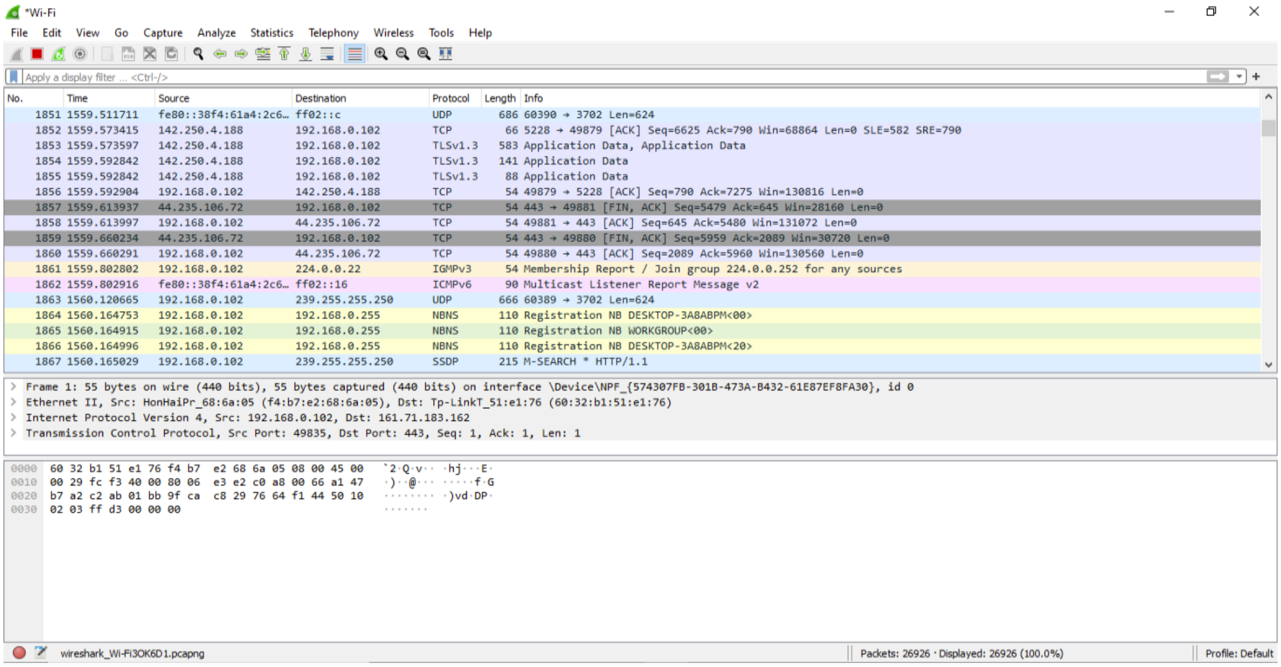
ROLL NO. :- TACO19108

YEAR AND DIV :- TE A

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

Solution :-

1. ESP :

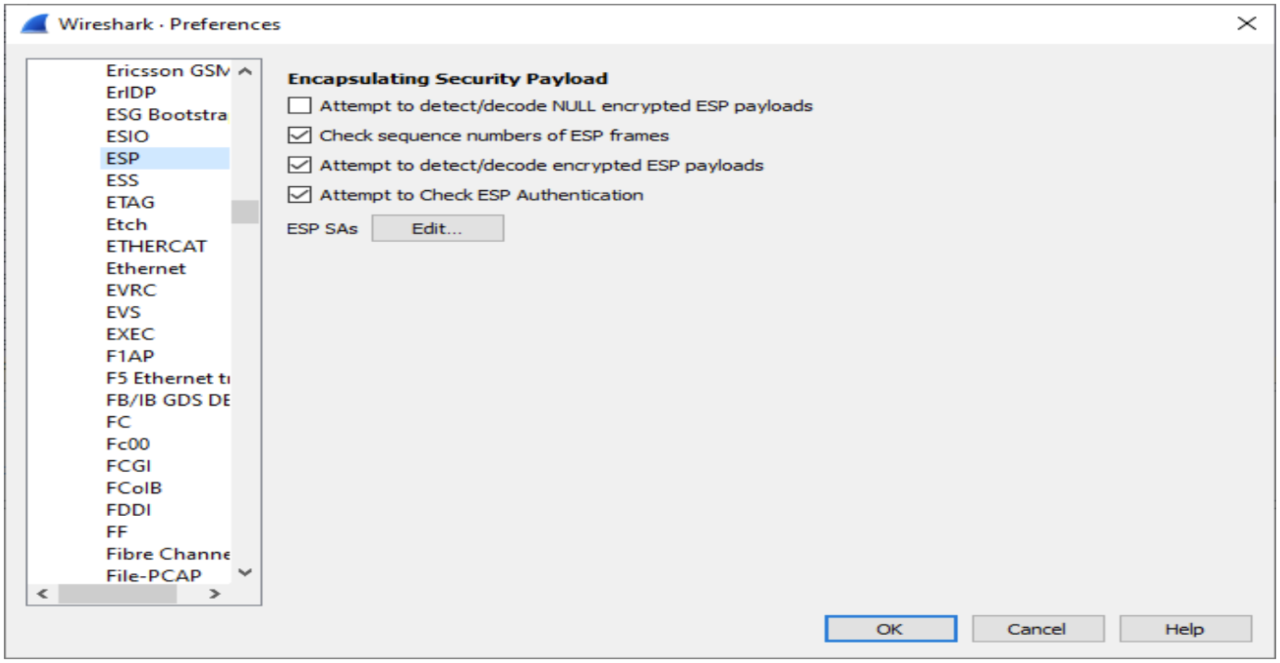

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source                    Destination        Protocol  Length Info
 1851 1559.511711   fe80::38f4:61a4:2c6…      ff02::c            UDP       686 60390 → 3702 Len=624
 1852 1559.573415   142.250.4.188             192.168.0.102      TCP        66 5228 → 49879 [ACK] Seq=6625 Ack=790 Win=68864 Len=0 SLE=582 SRE=790
 1853 1559.573597   142.250.4.188             192.168.0.102      TLSv1.3   583 Application Data, Application Data
 1854 1559.592842   142.250.4.188             192.168.0.102      TLSv1.3   141 Application Data
 1855 1559.592842   142.250.4.188             192.168.0.102      TLSv1.3    88 Application Data
 1856 1559.592904   192.168.0.102             142.250.4.188      TCP        54 49879 → 5228 [ACK] Seq=790 Ack=7275 Win=130816 Len=0
 1857 1559.613937   44.235.106.72             192.168.0.102      TCP        54 443 → 49881 [FIN, ACK] Seq=5479 Ack=645 Win=28160 Len=0
 1858 1559.613997   192.168.0.102             44.235.106.72      TCP        54 49881 → 443 [ACK] Seq=645 Ack=5480 Win=131072 Len=0
 1859 1559.660234   44.235.106.72             192.168.0.102      TCP        54 443 → 49880 [FIN, ACK] Seq=5959 Ack=2089 Win=30720 Len=0
 1860 1559.660291   192.168.0.102             44.235.106.72      TCP        54 49880 → 443 [ACK] Seq=2089 Ack=5960 Win=130560 Len=0
 1861 1559.802802   192.168.0.102             224.0.0.22         IGMPv3     54 Membership Report / Join group 224.0.0.252 for any sources
 1862 1559.802916   fe80::38f4:61a4:2c6…      ff02::16           ICMPv6     90 Multicast Listener Report Message v2
 1863 1560.120665   192.168.0.102             239.255.255.250    UDP       666 60389 → 3702 Len=624
 1864 1560.164753   192.168.0.102             192.168.0.255      NBNS      110 Registration NB DESKTOP-3A8ABPM<00>
 1865 1560.164915   192.168.0.102             192.168.0.255      NBNS      110 Registration NB WORKGROUP<00>
 1866 1560.164996   192.168.0.102             192.168.0.255      NBNS      110 Registration NB DESKTOP-3A8ABPM<20>
 1867 1560.165029   192.168.0.102             239.255.255.250    SSDP      215 M-SEARCH * HTTP/1.1
```

```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{574307FB-301B-473A-B432-61E87EF8FA30}, id 0
> Ethernet II, Src: HonHaiPr_68:6a:05 (f4:b7:e2:68:6a:05), Dst: Tp-LinkT_51:e1:76 (60:32:b1:51:e1:76)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 161.71.183.162
> Transmission Control Protocol, Src Port: 49835, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

```
0000  60 32 b1 51 e1 76 f4 b7  e2 68 6a 05 08 00 45 00   `2·Q·v·· ·hj···E·
0010  00 29 fc f3 40 00 80 06  e3 e2 c0 a8 00 66 a1 47   ·)··@··· ·····f·G
0020  b7 a2 c2 ab 01 bb 9f ca  c8 29 76 64 f1 44 50 10   ········ ·)vd·DP·
0030  02 03 ff d3 00 00 00                               ·······
```

wireshark_Wi-Fi3OK6D1.pcapng | Packets: 26926 · Displayed: 26926 (100.0%) | Profile: Default



Encapsulating Security Payload

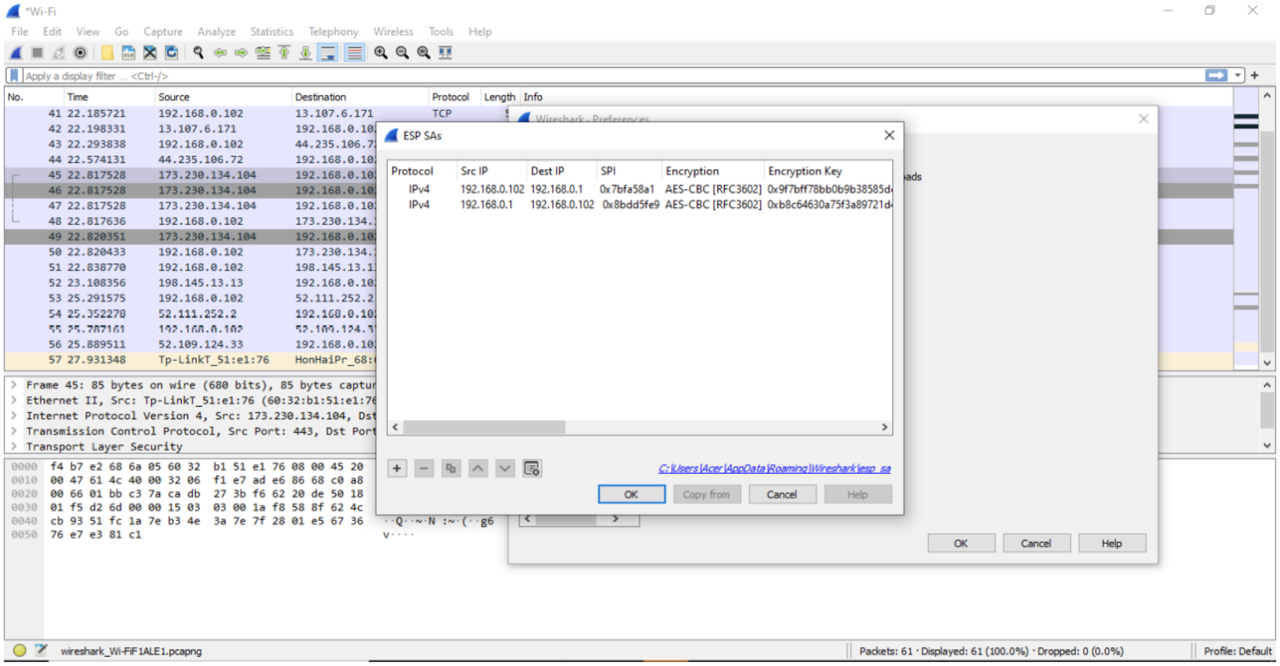
☐ Attempt to detect/decode NULL encrypted ESP payloads

☑ Check sequence numbers of ESP frames

☑ Attempt to detect/decode encrypted ESP payloads

☑ Attempt to Check ESP Authentication

ESP SAs Edit…



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Wireshark · Preferences
ESP SAs
ads

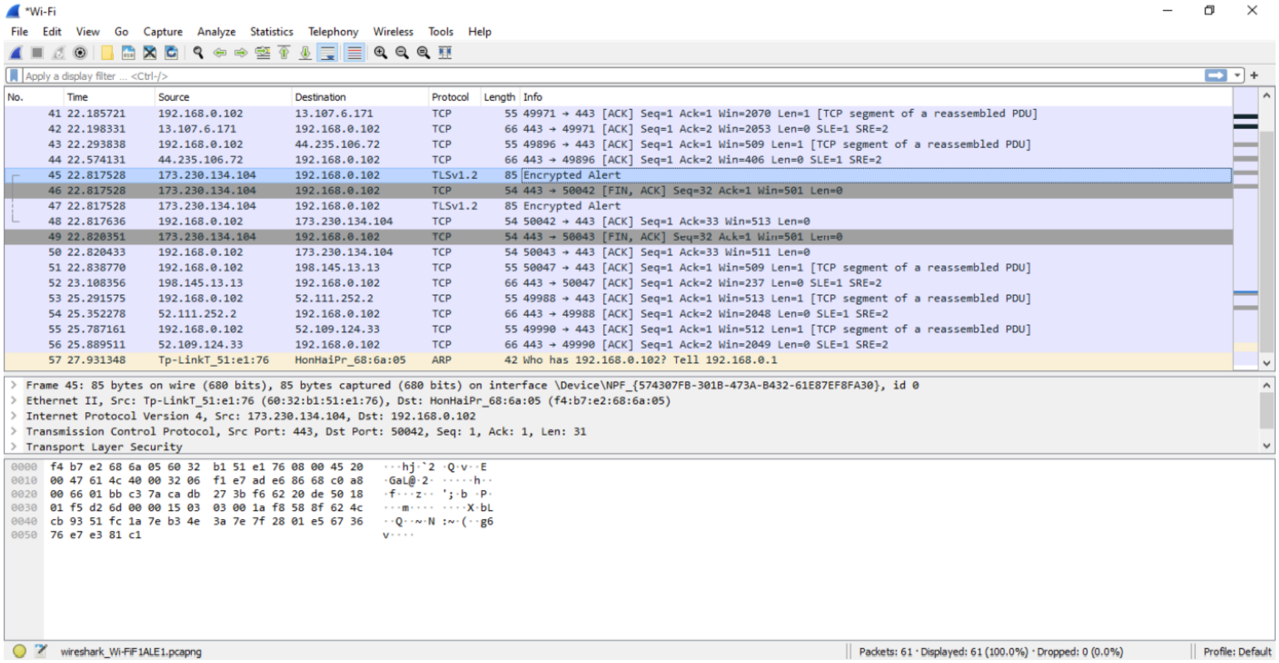
```
No.   Time       Source           Destination      Protocol Length Info
   41 22.185721  192.168.0.102    13.107.6.171     TCP
   42 22.198331  13.107.6.171     192.168.0.10
   43 22.293838  192.168.0.102    44.235.106.7
   44 22.574131  44.235.106.72    192.168.0.10
   45 22.817528  173.230.134.104  192.168.0.10
   46 22.817528  173.230.134.104  192.168.0.10
   47 22.817528  173.230.134.104  192.168.0.10
   48 22.817636  192.168.0.102    173.230.134.
   49 22.820351  173.230.134.104  192.168.0.10
   50 22.820433  192.168.0.102    173.230.134.
   51 22.838770  192.168.0.102    198.145.13.1
   52 23.108356  198.145.13.13    192.168.0.10
   53 25.291575  192.168.0.102    52.111.252.2
   54 25.352278  52.111.252.2     192.168.0.10
   55 25.787161  192.168.0.102    52.109.124.3
   56 25.889511  52.109.124.33    192.168.0.10
   57 27.931348  Tp-LinkT_51:e1:76 HonHaiPr_68:
```

```
> Frame 45: 85 bytes on wire (680 bits), 85 bytes captur
> Ethernet II, Src: Tp-LinkT_51:e1:76 (60:32:b1:51:e1:76
> Internet Protocol Version 4, Src: 173.230.134.104, Dst
> Transmission Control Protocol, Src Port: 443, Dst Port
> Transport Layer Security
```

```
0000  f4 b7 e2 68 6a 05 60 32  b1 51 e1 76 08 00 45 20
0010  00 47 61 4c 40 00 32 06  f1 e7 ad e6 86 68 c0 a8
0020  00 66 01 bb c3 7a ca db  27 3b f6 62 20 de 50 18
0030  01 f5 d2 6d 00 00 15 03  03 00 1a f8 58 8f 62 4c
0040  cb 93 51 fc 1a 7e b3 4e  3a 7e 7f 28 01 e5 67 36   ··Q··~·N :~·(··g6
0050  76 e7 e3 81 c1                                     v····
```

Protocol	Src IP	Dest IP	SPI	Encryption	Encryption Key
IPv4	192.168.0.102	192.168.0.1	0x7bfa58a1	AES-CBC [RFC3602]	0x9f7bff78bb0b9b38585d
IPv4	192.168.0.1	192.168.0.102	0x8bdd5fe9	AES-CBC [RFC3602]	0xb8c64630a75f3a89721d

wireshark_Wi-FiF1ALE1.pcapng Packets: 61 · Displayed: 61 (100.0%) · Dropped: 0 (0.0%) Profile: Default



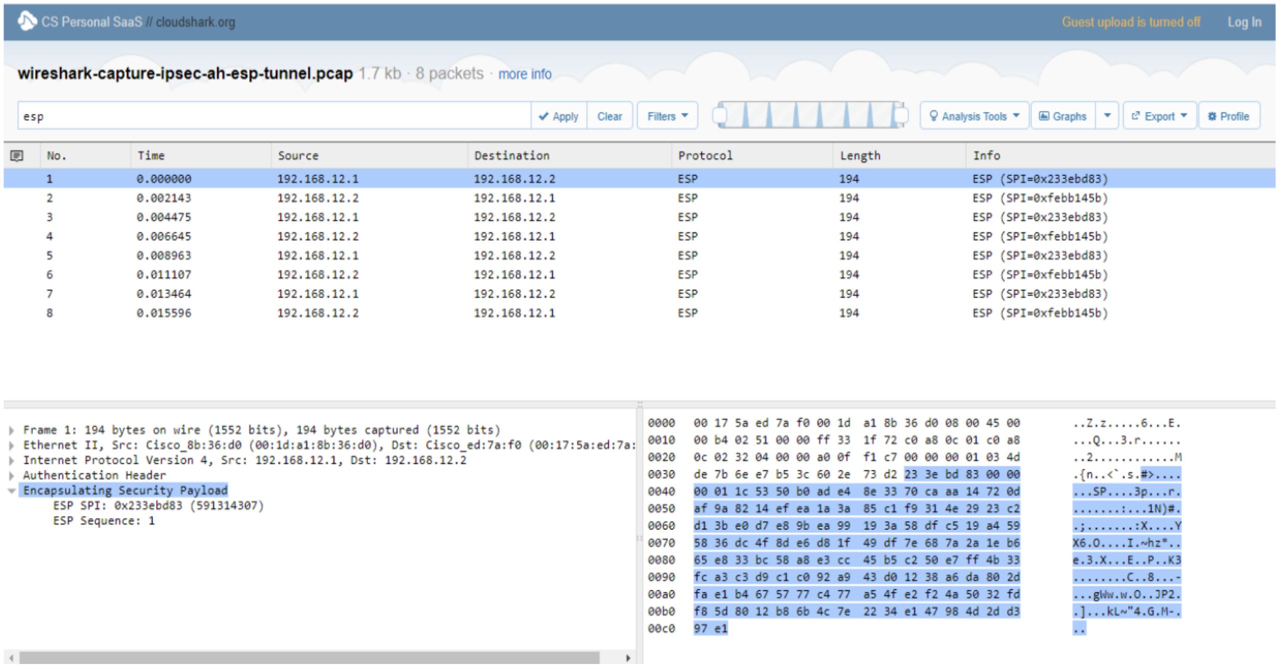
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time       Source           Destination      Protocol Length Info
   41 22.185721  192.168.0.102    13.107.6.171     TCP        55 49971 → 443 [ACK] Seq=1 Ack=1 Win=2070 Len=1 [TCP segment of a reassembled PDU]
   42 22.198331  13.107.6.171     192.168.0.102    TCP        66 443 → 49971 [ACK] Seq=1 Ack=2 Win=2053 Len=0 SLE=1 SRE=2
   43 22.293838  192.168.0.102    44.235.106.72    TCP        55 49896 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
   44 22.574131  44.235.106.72    192.168.0.102    TCP        66 443 → 49896 [ACK] Seq=1 Ack=2 Win=406 Len=0 SLE=1 SRE=2
   45 22.817528  173.230.134.104  192.168.0.102    TLSv1.2    85 Encrypted Alert
   46 22.817528  173.230.134.104  192.168.0.102    TCP        54 443 → 50042 [FIN, ACK] Seq=32 Ack=1 Win=501 Len=0
   47 22.817528  173.230.134.104  192.168.0.102    TLSv1.2    85 Encrypted Alert
   48 22.817636  192.168.0.102    173.230.134.104  TCP        54 50042 → 443 [ACK] Seq=1 Ack=33 Win=513 Len=0
   49 22.820351  173.230.134.104  192.168.0.102    TCP        54 443 → 50043 [FIN, ACK] Seq=32 Ack=1 Win=501 Len=0
   50 22.820433  192.168.0.102    173.230.134.104  TCP        54 50043 → 443 [ACK] Seq=1 Ack=33 Win=511 Len=0
   51 22.838770  192.168.0.102    198.145.13.13    TCP        55 50047 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
   52 23.108356  198.145.13.13    192.168.0.102    TCP        66 443 → 50047 [ACK] Seq=1 Ack=2 Win=237 Len=0 SLE=1 SRE=2
   53 25.291575  192.168.0.102    52.111.252.2     TCP        55 49988 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
   54 25.352278  52.111.252.2     192.168.0.102    TCP        66 443 → 49988 [ACK] Seq=1 Ack=2 Win=2048 Len=0 SLE=1 SRE=2
   55 25.787161  192.168.0.102    52.109.124.33    TCP        55 49990 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU]
   56 25.889511  52.109.124.33    192.168.0.102    TCP        66 443 → 49990 [ACK] Seq=1 Ack=2 Win=2049 Len=0 SLE=1 SRE=2
   57 27.931348  Tp-LinkT_51:e1:76 HonHaiPr_68:6a:05 ARP      42 Who has 192.168.0.102? Tell 192.168.0.1
```

```
> Frame 45: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{574307FB-301B-473A-B432-61E87EF8FA30}, id 0
> Ethernet II, Src: Tp-LinkT_51:e1:76 (60:32:b1:51:e1:76), Dst: HonHaiPr_68:6a:05 (f4:b7:e2:68:6a:05)
> Internet Protocol Version 4, Src: 173.230.134.104, Dst: 192.168.0.102
> Transmission Control Protocol, Src Port: 443, Dst Port: 50042, Seq: 1, Ack: 1, Len: 31
> Transport Layer Security
```

```
0000  f4 b7 e2 68 6a 05 60 32  b1 51 e1 76 08 00 45 20   ···hj·`2 ·Q·v··E
0010  00 47 61 4c 40 00 32 06  f1 e7 ad e6 86 68 c0 a8   ·GaL@·2· ·····h··
0020  00 66 01 bb c3 7a ca db  27 3b f6 62 20 de 50 18   ·f···z·· ';·b ·P·
0030  01 f5 d2 6d 00 00 15 03  03 00 1a f8 58 8f 62 4c   ···m···· ····X·bL
0040  cb 93 51 fc 1a 7e b3 4e  3a 7e 7f 28 01 e5 67 36   ··Q··~·N :~·(··g6
0050  76 e7 e3 81 c1                                     v····
```

wireshark_Wi-FiF1ALE1.pcapng Packets: 61 · Displayed: 61 (100.0%) · Dropped: 0 (0.0%) Profile: Default

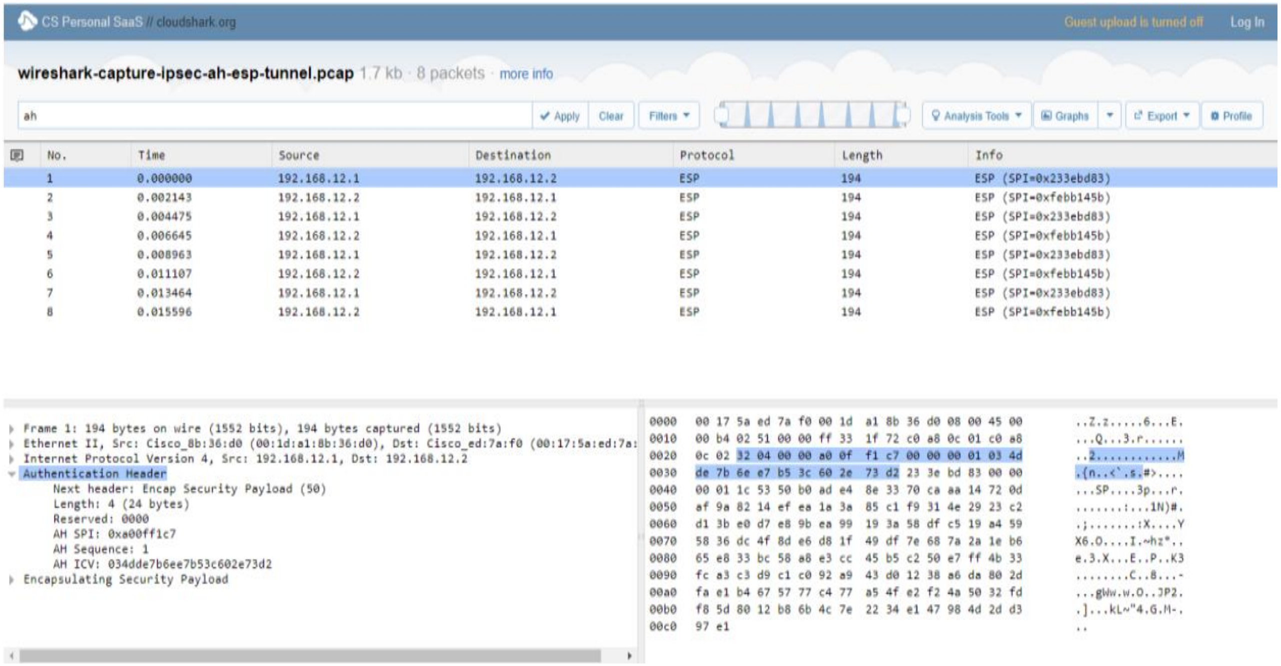

CS Personal SaaS // cloudshark.org
Guest upload is turned off
Log In
wireshark-capture-ipsec-ah-esp-tunnel.pcap 1.7 kb · 8 packets · more info
esp
Apply
Clear
Filters
Analysis Tools
Graphs
Export
Profile

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.12.1	192.168.12.2	ESP	194	ESP (SPI=0x233ebd83)
2	0.002143	192.168.12.2	192.168.12.1	ESP	194	ESP (SPI=0xfebb145b)
3	0.004475	192.168.12.1	192.168.12.2	ESP	194	ESP (SPI=0x233ebd83)
4	0.006645	192.168.12.2	192.168.12.1	ESP	194	ESP (SPI=0xfebb145b)
5	0.008963	192.168.12.1	192.168.12.2	ESP	194	ESP (SPI=0x233ebd83)
6	0.011107	192.168.12.2	192.168.12.1	ESP	194	ESP (SPI=0xfebb145b)
7	0.013464	192.168.12.1	192.168.12.2	ESP	194	ESP (SPI=0x233ebd83)
8	0.015596	192.168.12.2	192.168.12.1	ESP	194	ESP (SPI=0xfebb145b)

```
▸ Frame 1: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits)
▸ Ethernet II, Src: Cisco_8b:36:d0 (00:1d:a1:8b:36:d0), Dst: Cisco_ed:7a:f0 (00:17:5a:ed:7a:
▸ Internet Protocol Version 4, Src: 192.168.12.1, Dst: 192.168.12.2
▸ Authentication Header
▾ Encapsulating Security Payload
      ESP SPI: 0x233ebd83 (591314307)
      ESP Sequence: 1
```

```
0000   00 17 5a ed 7a f0 00 1d  a1 8b 36 d0 08 00 45 00     ..Z.z.....6...E.
0010   00 b4 02 51 00 00 ff 33  1f 72 c0 a8 0c 01 c0 a8     ...Q...3.r......
0020   0c 02 32 04 00 00 a0 0f  f1 c7 00 00 00 01 03 4d     ..2............M
0030   de 7b 6e e7 b5 3c 60 2e  73 d2 23 3e bd 83 00 00     .{n..<`.s.#>....
0040   00 01 1c 53 50 b0 ad e4  8e 33 70 ca aa 14 72 0d     ...SP....3p...r.
0050   af 9a 82 14 ef ea 1a 3a  85 c1 f9 31 4e 29 23 c2     .......:...1N)#.
0060   d1 3b e0 d7 e8 9b ea 99  19 3a 58 df c5 19 a4 59     .;.......:X....Y
0070   58 36 dc 4f 8d e6 d8 1f  49 df 7e 68 7a 2a 1e b6     X6.O....I.~hz*..
0080   65 e8 33 bc 58 a8 e3 cc  45 b5 c2 50 e7 ff 4b 33     e.3.X...E..P..K3
0090   fc a3 c3 d9 c1 c0 92 a9  43 d0 12 38 a6 da 80 2d     ........C..8...-
00a0   fa e1 b4 67 57 77 c4 77  a5 4f e2 f2 4a 50 32 fd     ...gWw.w.O..JP2.
00b0   f8 5d 80 12 b8 6b 4c 7e  22 34 e1 47 98 4d 2d d3     .]...kL~"4.G.M-.
00c0   97 e1                                                ..
```

2. AH :


CS Personal SaaS // cloudshark.org
Guest upload is turned off
Log In
wireshark-capture-ipsec-ah-esp-tunnel.pcap 1.7 kb · 8 packets · more info
ah
Apply
Clear
Filters
Analysis Tools
Graphs
Export
Profile

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.12.1	192.168.12.2	ESP	194	ESP (SPI=0x233ebd83)
2	0.002143	192.168.12.2	192.168.12.1	ESP	194	ESP (SPI=0xfebb145b)
3	0.004475	192.168.12.1	192.168.12.2	ESP	194	ESP (SPI=0x233ebd83)
4	0.006645	192.168.12.2	192.168.12.1	ESP	194	ESP (SPI=0xfebb145b)
5	0.008963	192.168.12.1	192.168.12.2	ESP	194	ESP (SPI=0x233ebd83)
6	0.011107	192.168.12.2	192.168.12.1	ESP	194	ESP (SPI=0xfebb145b)
7	0.013464	192.168.12.1	192.168.12.2	ESP	194	ESP (SPI=0x233ebd83)
8	0.015596	192.168.12.2	192.168.12.1	ESP	194	ESP (SPI=0xfebb145b)

```
▸ Frame 1: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits)
▸ Ethernet II, Src: Cisco_8b:36:d0 (00:1d:a1:8b:36:d0), Dst: Cisco_ed:7a:f0 (00:17:5a:ed:7a:
▸ Internet Protocol Version 4, Src: 192.168.12.1, Dst: 192.168.12.2
▾ Authentication Header
      Next header: Encap Security Payload (50)
      Length: 4 (24 bytes)
      Reserved: 0000
      AH SPI: 0xa00ff1c7
      AH Sequence: 1
      AH ICV: 034dde7b6ee7b53c602e73d2
▸ Encapsulating Security Payload
```

```
0000   00 17 5a ed 7a f0 00 1d  a1 8b 36 d0 08 00 45 00     ..Z.z.....6...E.
0010   00 b4 02 51 00 00 ff 33  1f 72 c0 a8 0c 01 c0 a8     ...Q...3.r......
0020   0c 02 32 04 00 00 a0 0f  f1 c7 00 00 00 01 03 4d     ..2............M
0030   de 7b 6e e7 b5 3c 60 2e  73 d2 23 3e bd 83 00 00     .{n..<`.s.#>....
0040   00 01 1c 53 50 b0 ad e4  8e 33 70 ca aa 14 72 0d     ...SP....3p...r.
0050   af 9a 82 14 ef ea 1a 3a  85 c1 f9 31 4e 29 23 c2     .......:...1N)#.
0060   d1 3b e0 d7 e8 9b ea 99  19 3a 58 df c5 19 a4 59     .;.......:X....Y
0070   58 36 dc 4f 8d e6 d8 1f  49 df 7e 68 7a 2a 1e b6     X6.O....I.~hz*..
0080   65 e8 33 bc 58 a8 e3 cc  45 b5 c2 50 e7 ff 4b 33     e.3.X...E..P..K3
0090   fc a3 c3 d9 c1 c0 92 a9  43 d0 12 38 a6 da 80 2d     ........C..8...-
00a0   fa e1 b4 67 57 77 c4 77  a5 4f e2 f2 4a 50 32 fd     ...gWw.w.O..JP2.
00b0   f8 5d 80 12 b8 6b 4c 7e  22 34 e1 47 98 4d 2d d3     .]...kL~"4.G.M-.
00c0   97 e1                                                ..
```