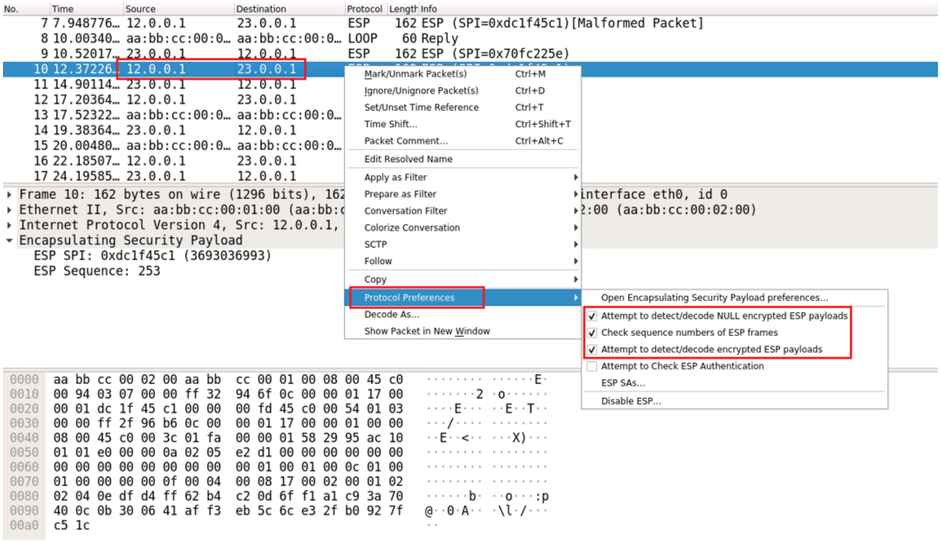
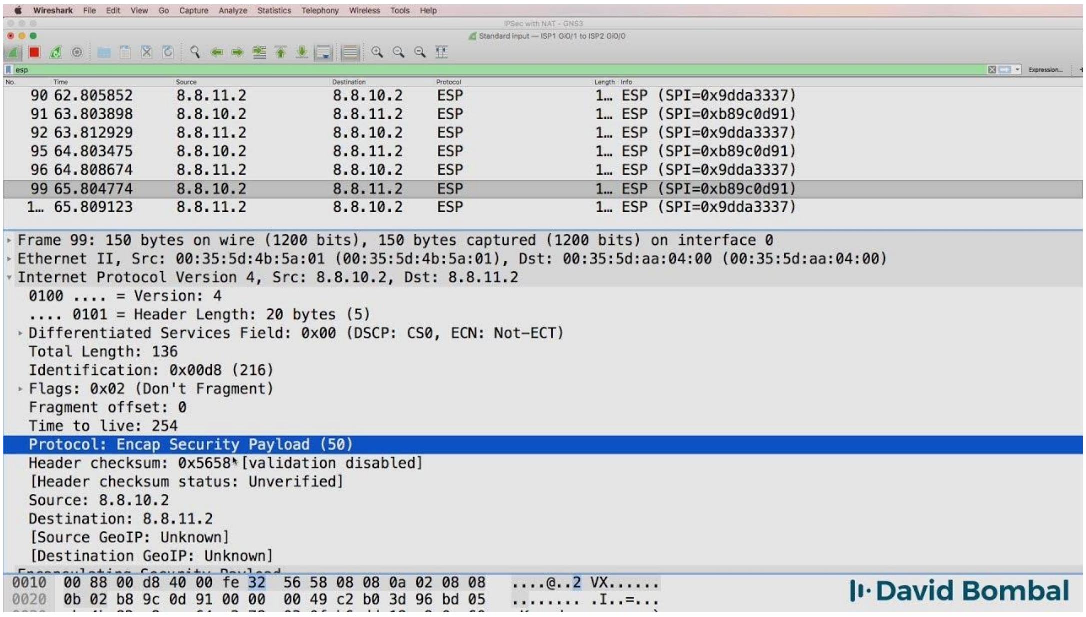


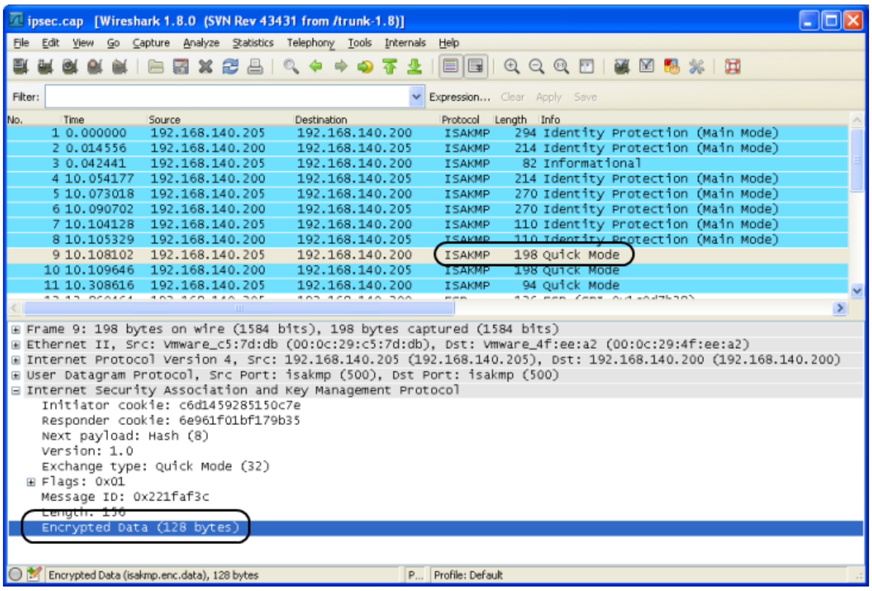
```
No.  Time        Source           Destination      Protocol Length Info
   7 7.948776…  12.0.0.1         23.0.0.1         ESP      162 ESP (SPI=0xdc1f45c1)[Malformed Packet]
   8 10.00340…  aa:bb:cc:00:0…   aa:bb:cc:00:0…   LOOP      60 Reply
   9 10.52017…  23.0.0.1         12.0.0.1         ESP      162 ESP (SPI=0x70fc225e)
  10 12.37226…  12.0.0.1         23.0.0.1
  11 14.90114…  23.0.0.1         12.0.0.1
  12 17.20364…  12.0.0.1         23.0.0.1
  13 17.52322…  aa:bb:cc:00:0…   aa:bb:cc:00:0…
  14 19.38364…  23.0.0.1         12.0.0.1
  15 20.00480…  aa:bb:cc:00:0…   aa:bb:cc:00:0…
  16 22.18507…  12.0.0.1         23.0.0.1
  17 24.19585…  23.0.0.1         12.0.0.1

▸ Frame 10: 162 bytes on wire (1296 bits), 162                    interface eth0, id 0
▸ Ethernet II, Src: aa:bb:cc:00:01:00 (aa:bb:c                    2:00 (aa:bb:cc:00:02:00)
▸ Internet Protocol Version 4, Src: 12.0.0.1,
▾ Encapsulating Security Payload
    ESP SPI: 0xdc1f45c1 (3693036993)
    ESP Sequence: 253

0000  aa bb cc 00 02 00 aa bb  cc 00 01 00 08 00 45 c0   ········ ······E·
0010  00 94 03 07 00 00 ff 32  94 6f 0c 00 00 01 17 00   ·······2 ·o······
0020  00 01 dc 1f 45 c1 00 00  00 fd 45 c0 00 54 01 03   ····E··· ··E··T··
0030  00 00 ff 2f 96 b6 0c 00  00 01 17 00 00 01 00 00   ···/···· ········
0040  08 00 45 c0 00 3c 01 fa  00 00 01 58 29 95 ac 10   ··E··<·· ···X)···
0050  01 01 e0 00 00 0a 02 05  e2 d1 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 01 00 01 00 0c 01 00   ········ ········
0070  01 00 00 00 00 0f 00 04  00 08 17 00 02 00 01 02   ········ ········
0080  02 04 0e df d4 ff 62 b4  c2 0d 6f f1 a1 c9 3a 70   ······b· ··o···:p
0090  40 0c 0b 30 06 41 af f3  eb 5c 6c e3 2f b0 92 7f   @··0·A·· ·\l·/···
00a0  c5 1c                                              ··
```

Mark/Unmark Packet(s) Ctrl+M
Ignore/Unignore Packet(s) Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift… Ctrl+Shift+T
Packet Comment… Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As…
Show Packet in New Window
Open Encapsulating Security Payload preferences…
☑ 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…
Disable ESP…



Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
IPSec with NAT - GNS3
Standard input — ISP1 Gi0/1 to ISP2 Gi0/0
esp
Expression…
David Bombal

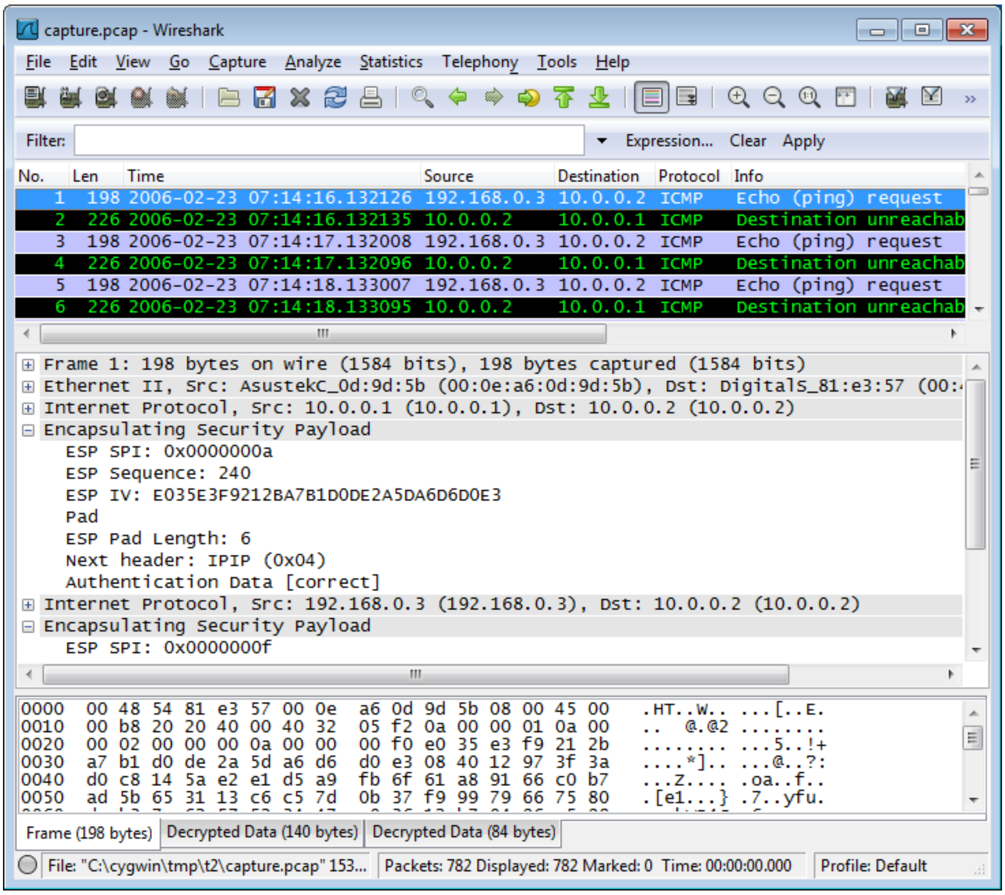
```
No.  Time       Source     Destination  Protocol  Length Info
  90 62.805852  8.8.11.2   8.8.10.2     ESP       1…  ESP (SPI=0x9dda3337)
  91 63.803898  8.8.10.2   8.8.11.2     ESP       1…  ESP (SPI=0xb89c0d91)
  92 63.812929  8.8.11.2   8.8.10.2     ESP       1…  ESP (SPI=0x9dda3337)
  95 64.803475  8.8.10.2   8.8.11.2     ESP       1…  ESP (SPI=0xb89c0d91)
  96 64.808674  8.8.11.2   8.8.10.2     ESP       1…  ESP (SPI=0x9dda3337)
  99 65.804774  8.8.10.2   8.8.11.2     ESP       1…  ESP (SPI=0xb89c0d91)
  1… 65.809123  8.8.11.2   8.8.10.2     ESP       1…  ESP (SPI=0x9dda3337)

▸ Frame 99: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
▸ Ethernet II, Src: 00:35:5d:4b:5a:01 (00:35:5d:4b:5a:01), Dst: 00:35:5d:aa:04:00 (00:35:5d:aa:04:00)
▾ Internet Protocol Version 4, Src: 8.8.10.2, Dst: 8.8.11.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 136
    Identification: 0x00d8 (216)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 254
    Protocol: Encap Security Payload (50)
    Header checksum: 0x5658 [validation disabled]
    [Header checksum status: Unverified]
    Source: 8.8.10.2
    Destination: 8.8.11.2
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]

0010  00 88 00 d8 40 00 fe 32  56 58 08 08 0a 02 08 08   ....@..2 VX......
0020  0b 02 b8 9c 0d 91 00 00  00 49 c2 b0 3d 96 bd 05   ........ .I..=...
```


ipsec.cap [Wireshark 1.8.0 (SVN Rev 43431 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time       Source           Destination      Protocol Length Info
   1 0.000000   192.168.140.205  192.168.140.200  ISAKMP   294 Identity Protection (Main Mode)
   2 0.014556   192.168.140.200  192.168.140.205  ISAKMP   214 Identity Protection (Main Mode)
   3 0.042441   192.168.140.205  192.168.140.200  ISAKMP    82 Informational
   4 10.054177  192.168.140.200  192.168.140.205  ISAKMP   214 Identity Protection (Main Mode)
   5 10.073018  192.168.140.205  192.168.140.200  ISAKMP   270 Identity Protection (Main Mode)
   6 10.090702  192.168.140.200  192.168.140.205  ISAKMP   270 Identity Protection (Main Mode)
   7 10.104128  192.168.140.205  192.168.140.200  ISAKMP   110 Identity Protection (Main Mode)
   8 10.105329  192.168.140.200  192.168.140.205  ISAKMP   110 Identity Protection (Main Mode)
   9 10.108102  192.168.140.205  192.168.140.200  ISAKMP   198 Quick Mode
  10 10.109646  192.168.140.200  192.168.140.205  ISAKMP   198 Quick Mode
  11 10.308616  192.168.140.205  192.168.140.200  ISAKMP    94 Quick Mode
```

```
⊞ Frame 9: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits)
⊞ Ethernet II, Src: Vmware_c5:7d:db (00:0c:29:c5:7d:db), Dst: Vmware_4f:ee:a2 (00:0c:29:4f:ee:a2)
⊞ Internet Protocol Version 4, Src: 192.168.140.205 (192.168.140.205), Dst: 192.168.140.200 (192.168.140.200)
⊞ User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
⊟ Internet Security Association and Key Management Protocol
    Initiator cookie: c6d1459285150c7e
    Responder cookie: 6e961f01bf179b35
    Next payload: Hash (8)
    Version: 1.0
    Exchange type: Quick Mode (32)
  ⊞ Flags: 0x01
    Message ID: 0x221faf3c
    Length: 156
    Encrypted Data (128 bytes)
```

Encrypted Data (isakmp.enc.data), 128 bytes | P... | Profile: Default


capture.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. Len Time                       Source       Destination Protocol Info
  1 198 2006-02-23 07:14:16.132126 192.168.0.3  10.0.0.2    ICMP     Echo (ping) request
  2 226 2006-02-23 07:14:16.132135 10.0.0.2     10.0.0.1    ICMP     Destination unreachab
  3 198 2006-02-23 07:14:17.132008 192.168.0.3  10.0.0.2    ICMP     Echo (ping) request
  4 226 2006-02-23 07:14:17.132096 10.0.0.2     10.0.0.1    ICMP     Destination unreachab
  5 198 2006-02-23 07:14:18.133007 192.168.0.3  10.0.0.2    ICMP     Echo (ping) request
  6 226 2006-02-23 07:14:18.133095 10.0.0.2     10.0.0.1    ICMP     Destination unreachab
```

```
⊞ Frame 1: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits)
⊞ Ethernet II, Src: AsustekC_0d:9d:5b (00:0e:a6:0d:9d:5b), Dst: Digitals_81:e3:57 (00:
⊞ Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.2 (10.0.0.2)
⊟ Encapsulating Security Payload
    ESP SPI: 0x0000000a
    ESP Sequence: 240
    ESP IV: E035E3F9212BA7B1D0DE2A5DA6D6D0E3
    Pad
    ESP Pad Length: 6
    Next header: IPIP (0x04)
    Authentication Data [correct]
⊞ Internet Protocol, Src: 192.168.0.3 (192.168.0.3), Dst: 10.0.0.2 (10.0.0.2)
⊟ Encapsulating Security Payload
    ESP SPI: 0x0000000f
```

```
0000  00 48 54 81 e3 57 00 0e  a6 0d 9d 5b 08 00 45 00   .HT..W.. ...[..E.
0010  00 b8 20 20 40 00 40 32  05 f2 0a 00 00 01 0a 00   ..  @.@2 ........
0020  00 02 00 00 00 0a 00 00  00 f0 e0 35 e3 f9 21 2b   ........ ...5..!+
0030  a7 b1 d0 de 2a 5d a6 d6  d0 e3 08 40 12 97 3f 3a   ....*]..  ...@..?:
0040  d0 c8 14 5a e2 e1 d5 a9  fb 6f 61 a8 91 66 c0 b7   ...Z.... .oa..f..
0050  ad 5b 65 31 13 c6 c5 7d  0b 37 f9 99 79 66 75 80   .[e1...} .7..yfu.
```

File: "C:\cygwin\tmp\t2\capture.pcap" 153... | Packets: 782 Displayed: 782 Marked: 0 Time: 00:00:00.000 | Profile: Default