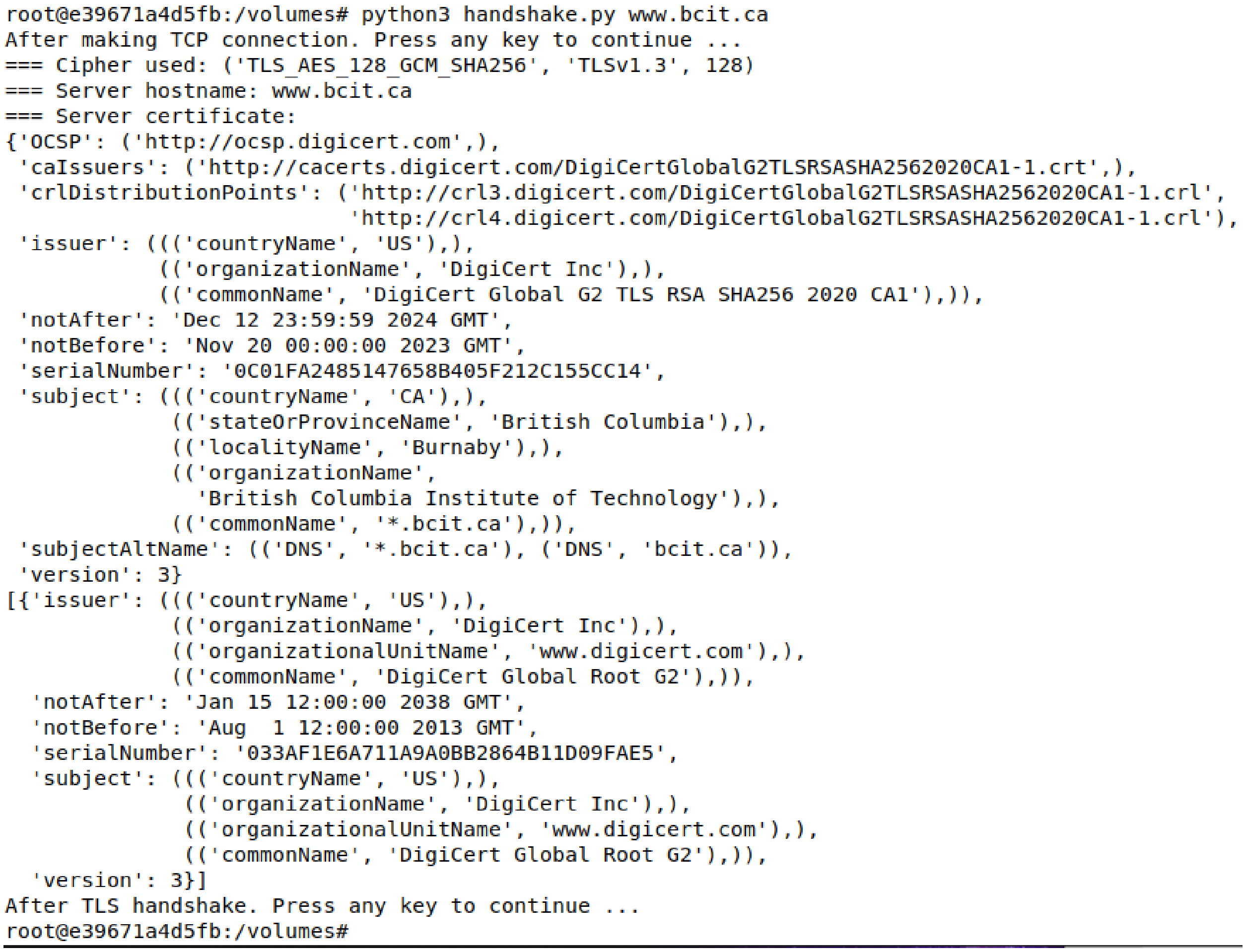
ACIT 4630 – Assignment 3 – Transport Layer Security

Markus Afonso
Set C
March 25, 2024

Running handshake.py



```
root@e39671a4d5fb:/volumes# python3 handshake.py www.bcit.ca
After making TCP connection. Press any key to continue ...
=== Cipher used: ('TLS_AES_128_GCM_SHA256', 'TLSv1.3', 128)
=== Server hostname: www.bcit.ca
=== Server certificate:
{'OCSP': ('http://ocsp.digicert.com',),
 'caIssuers': ('http://cacerts.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-1.crt',),
 'crlDistributionPoints': ('http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-1.crl',
                           'http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-1.crl'),
 'issuer': ((('countryName', 'US'),),
            (('organizationName', 'DigiCert Inc'),),
            (('commonName', 'DigiCert Global G2 TLS RSA SHA256 2020 CA1'),)),
 'notAfter': 'Dec 12 23:59:59 2024 GMT',
 'notBefore': 'Nov 20 00:00:00 2023 GMT',
 'serialNumber': '0C01FA2485147658B405F212C155CC14',
 'subject': ((('countryName', 'CA'),),
             (('stateOrProvinceName', 'British Columbia'),),
             (('localityName', 'Burnaby'),),
             (('organizationName',
               'British Columbia Institute of Technology'),),
             (('commonName', '*.bcit.ca'),)),
 'subjectAltName': (('DNS', '*.bcit.ca'), ('DNS', 'bcit.ca')),
 'version': 3}
[{'issuer': ((('countryName', 'US'),),
             (('organizationName', 'DigiCert Inc'),),
             (('organizationalUnitName', 'www.digicert.com'),),
             (('commonName', 'DigiCert Global Root G2'),)),
  'notAfter': 'Jan 15 12:00:00 2038 GMT',
  'notBefore': 'Aug  1 12:00:00 2013 GMT',
  'serialNumber': '033AF1E6A711A9A0BB2864B11D09FAE5',
  'subject': ((('countryName', 'US'),),
              (('organizationName', 'DigiCert Inc'),),
              (('organizationalUnitName', 'www.digicert.com'),),
              (('commonName', 'DigiCert Global Root G2'),)),
  'version': 3}]
After TLS handshake. Press any key to continue ...
root@e39671a4d5fb:/volumes#
```

Q1. What is the cipher used between the client and the server?

The cypher used is TLS-AES-128-GCM-SHA256, TLSv1.3, 128.

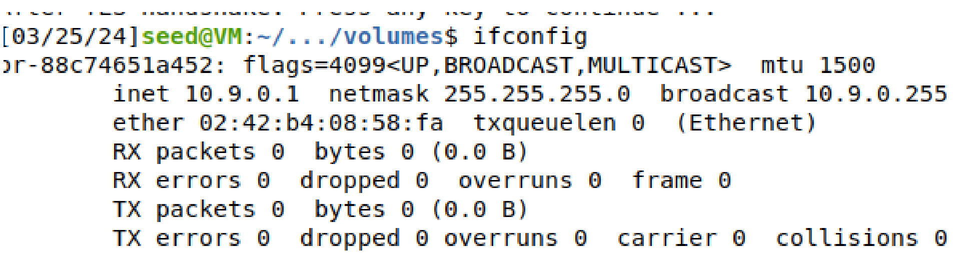
Q2. What is the server's public certificate used for after the client verifies the server's identity and its public key?

After the client verifies the server's identity and its public key using the server's public certificate, the certificate is primarily used for encryption and authentication purposes during the TLS handshake. Once the server's identity is verified, its public key is used by the client to establish a secure communication channel. This includes encrypting data sent from the client to the server and decrypting data received from the server. Additionally, the server's public certificate helps ensure the integrity and authenticity of the communication by allowing the client to verify that it is indeed communicating with the intended server and not an impostor.

Explain the purpose of cadir = '/etc/ssl/certs':

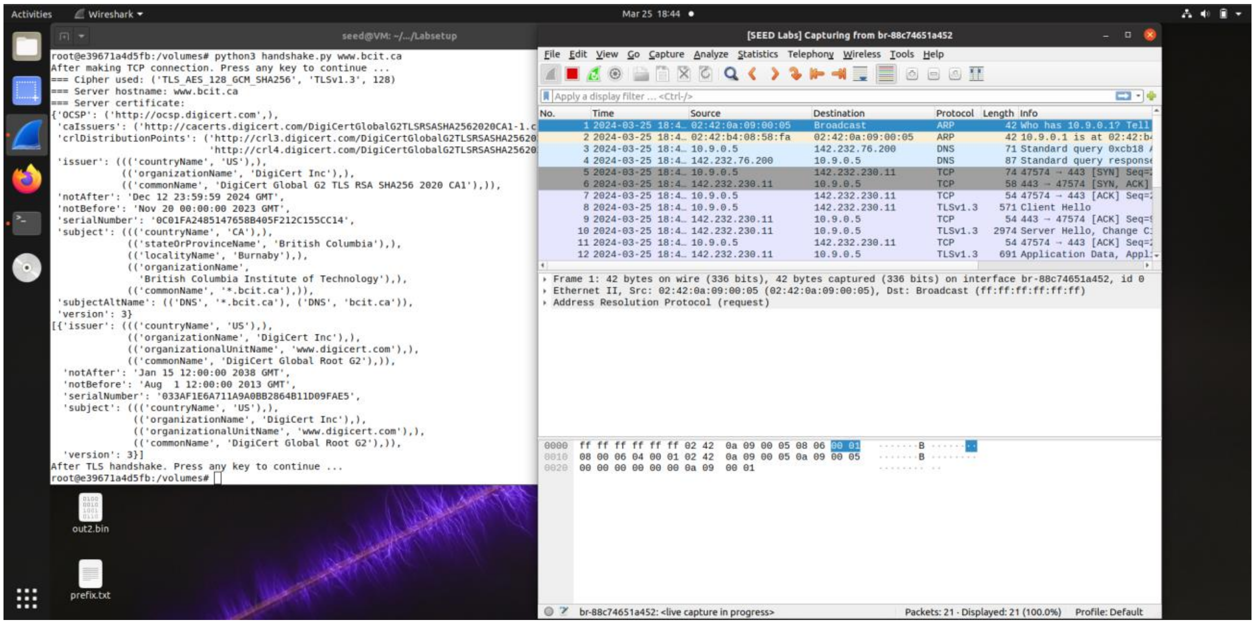
In the handshake.py code, cadir is set to '/etc/ssl/certs', storing the directory where trusted CA certificates are kept. These certificates are used for verifying the authenticity of the server's certificate during the TLS handshake process.

Using ifconfig:



```
After TLS handshake. Press any key to continue ...
[03/25/24]seed@VM:~/.../volumes$ ifconfig
br-88c74651a452: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 10.9.0.1  netmask 255.255.255.0  broadcast 10.9.0.255
        ether 02:42:b4:08:58:fa  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Running handshake.py:

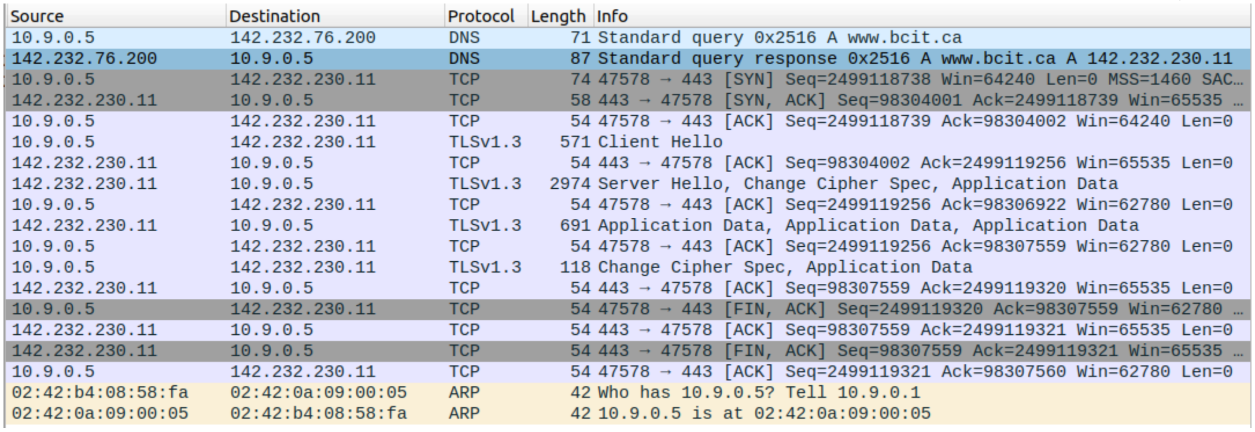


Activities
Wireshark
Mar 25 18:44
seed@VM: ~/.../Labsetup
[SEED Labs] Capturing from br-88c74651a452
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
out2.bin
prefix.txt

```
root@e39671a4d5fb:/volumes# python3 handshake.py www.bcit.ca
After making TCP connection. Press any key to continue ...
=== Cipher used: ('TLS_AES_128_GCM_SHA256', 'TLSv1.3', 128)
=== Server hostname: www.bcit.ca
=== Server certificate:
{'OCSP': ('http://ocsp.digicert.com',),
 'caIssuers': ('http://cacerts.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-1.c
 'crlDistributionPoints': ('http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA25620
                           'http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA25620
 'issuer': ((('countryName', 'US'),),
            (('organizationName', 'DigiCert Inc'),),
            (('commonName', 'DigiCert Global G2 TLS RSA SHA256 2020 CA1'),)),
 'notAfter': 'Dec 12 23:59:59 2024 GMT',
 'notBefore': 'Nov 20 00:00:00 2023 GMT',
 'serialNumber': '0C01FA2485147658B405F212C155CC14',
 'subject': ((('countryName', 'CA'),),
             (('stateOrProvinceName', 'British Columbia'),),
             (('localityName', 'Burnaby'),),
             (('organizationName',
               'British Columbia Institute of Technology'),),
             (('commonName', '*.bcit.ca'),)),
 'subjectAltName': (('DNS', '*.bcit.ca'), ('DNS', 'bcit.ca')),
 'version': 3}
[{'issuer': ((('countryName', 'US'),),
             (('organizationName', 'DigiCert Inc'),),
             (('organizationalUnitName', 'www.digicert.com'),),
             (('commonName', 'DigiCert Global Root G2'),)),
  'notAfter': 'Jan 15 12:00:00 2038 GMT',
  'notBefore': 'Aug  1 12:00:00 2013 GMT',
  'serialNumber': '033AF1E6A711A9A0BB2864B11D09FAE5',
  'subject': ((('countryName', 'US'),),
              (('organizationName', 'DigiCert Inc'),),
              (('organizationalUnitName', 'www.digicert.com'),),
              (('commonName', 'DigiCert Global Root G2'),)),
  'version': 3}]
After TLS handshake. Press any key to continue ...
root@e39671a4d5fb:/volumes# 
```

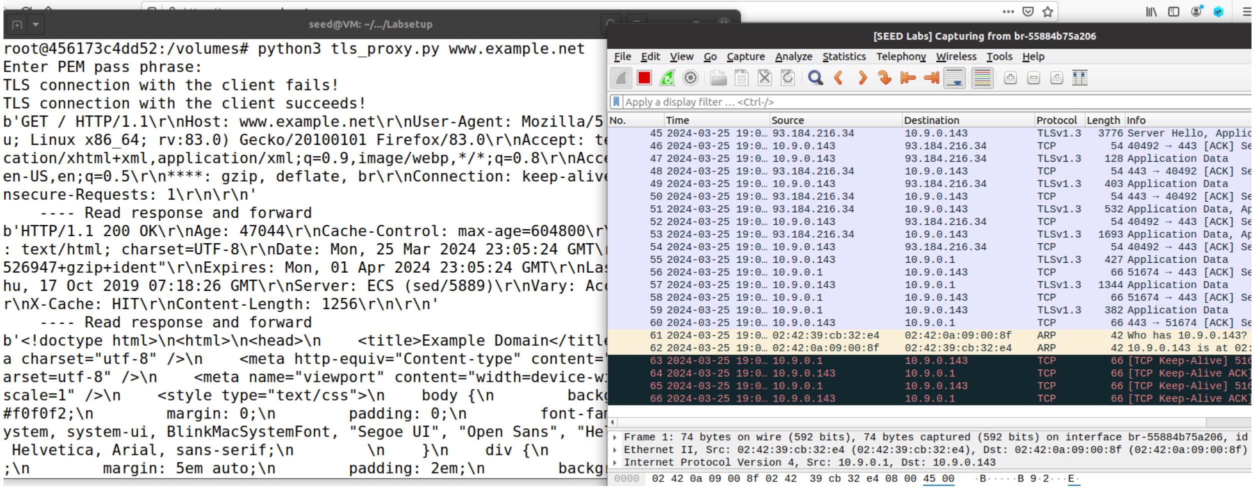
```
No.   Time             Source              Destination         Protocol  Length Info
    1 2024-03-25 18:4… 02:42:0a:09:00:05   Broadcast           ARP          42 Who has 10.9.0.1? Tell
    2 2024-03-25 18:4… 02:42:b4:08:58:fa   02:42:0a:09:00:05   ARP          42 10.9.0.1 is at 02:42:b
    3 2024-03-25 18:4… 10.9.0.5            142.232.76.200      DNS          71 Standard query 0xcb18 
    4 2024-03-25 18:4… 142.232.76.200      10.9.0.5            DNS          87 Standard query response
    5 2024-03-25 18:4… 10.9.0.5            142.232.230.11      TCP          74 47574 → 443 [SYN] Seq=
    6 2024-03-25 18:4… 142.232.230.11      10.9.0.5            TCP          58 443 → 47574 [SYN, ACK]
    7 2024-03-25 18:4… 10.9.0.5            142.232.230.11      TCP          54 47574 → 443 [ACK] Seq=
    8 2024-03-25 18:4… 10.9.0.5            142.232.230.11      TLSv1.3     571 Client Hello
    9 2024-03-25 18:4… 142.232.230.11      10.9.0.5            TCP          54 443 → 47574 [ACK] Seq=
   10 2024-03-25 18:4… 142.232.230.11      10.9.0.5            TLSv1.3    2974 Server Hello, Change C
   11 2024-03-25 18:4… 10.9.0.5            142.232.230.11      TCP          54 47574 → 443 [ACK] Seq=
   12 2024-03-25 18:4… 142.232.230.11      10.9.0.5            TLSv1.3     691 Application Data, Appl

▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface br-88c74651a452, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 02 42  0a 09 00 05 08 06 00 01   ·······B ········
0010  08 00 06 04 00 01 02 42  0a 09 00 05 0a 09 00 05   ·······B ········
0020  00 00 00 00 00 00 0a 09  00 01                     ········ ··

br-88c74651a452: <live capture in progress>          Packets: 21 · Displayed: 21 (100.0%)    Profile: Default
```

We can clearly see the handshake process, with the 'Client Hello' , 'Server hello', etc.. in the info column:



Source	Destination	Protocol	Length	Info
10.9.0.5	142.232.76.200	DNS	71	Standard query 0x2516 A www.bcit.ca
142.232.76.200	10.9.0.5	DNS	87	Standard query response 0x2516 A www.bcit.ca A 142.232.230.11
10.9.0.5	142.232.230.11	TCP	74	47578 → 443 [SYN] Seq=2499118738 Win=64240 Len=0 MSS=1460 SAC…
142.232.230.11	10.9.0.5	TCP	58	443 → 47578 [SYN, ACK] Seq=98304001 Ack=2499118739 Win=65535 …
10.9.0.5	142.232.230.11	TCP	54	47578 → 443 [ACK] Seq=2499118739 Ack=98304002 Win=64240 Len=0
10.9.0.5	142.232.230.11	TLSv1.3	571	Client Hello
142.232.230.11	10.9.0.5	TCP	54	443 → 47578 [ACK] Seq=98304002 Ack=2499119256 Win=65535 Len=0
142.232.230.11	10.9.0.5	TLSv1.3	2974	Server Hello, Change Cipher Spec, Application Data
10.9.0.5	142.232.230.11	TCP	54	47578 → 443 [ACK] Seq=2499119256 Ack=98306922 Win=62780 Len=0
142.232.230.11	10.9.0.5	TLSv1.3	691	Application Data, Application Data, Application Data
10.9.0.5	142.232.230.11	TCP	54	47578 → 443 [ACK] Seq=2499119256 Ack=98307559 Win=62780 Len=0
10.9.0.5	142.232.230.11	TLSv1.3	118	Change Cipher Spec, Application Data
142.232.230.11	10.9.0.5	TCP	54	443 → 47578 [ACK] Seq=98307559 Ack=2499119320 Win=65535 Len=0
10.9.0.5	142.232.230.11	TCP	54	47578 → 443 [FIN, ACK] Seq=2499119320 Ack=98307559 Win=62780 …
142.232.230.11	10.9.0.5	TCP	54	443 → 47578 [ACK] Seq=98307559 Ack=2499119321 Win=65535 Len=0
142.232.230.11	10.9.0.5	TCP	54	443 → 47578 [FIN, ACK] Seq=98307559 Ack=2499119321 Win=65535 …
10.9.0.5	142.232.230.11	TCP	54	47578 → 443 [ACK] Seq=2499119321 Ack=98307560 Win=62780 Len=0
02:42:b4:08:58:fa	02:42:0a:09:00:05	ARP	42	Who has 10.9.0.5? Tell 10.9.0.1
02:42:0a:09:00:05	02:42:b4:08:58:fa	ARP	42	10.9.0.5 is at 02:42:0a:09:00:05

Proxy container is seeing the communication:



```
root@456173c4dd52:/volumes# python3 tls_proxy.py www.example.net
Enter PEM pass phrase:
TLS connection with the client fails!
TLS connection with the client succeeds!
b'GET / HTTP/1.1\r\nHost: www.example.net\r\nUser-Agent: Mozilla/5
u; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0\r\nAccept: te
cation/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\nAcce
en-US,en;q=0.5\r\n****: gzip, deflate, br\r\nConnection: keep-alive
nsecure-Requests: 1\r\n\r\n'
    ---- Read response and forward
b'HTTP/1.1 200 OK\r\nAge: 47044\r\nCache-Control: max-age=604800\r\
: text/html; charset=UTF-8\r\nDate: Mon, 25 Mar 2024 23:05:24 GMT\r
526947+gzip+ident"\r\nExpires: Mon, 01 Apr 2024 23:05:24 GMT\r\nLas
hu, 17 Oct 2019 07:18:26 GMT\r\nServer: ECS (sed/5889)\r\nVary: Acc
r\nX-Cache: HIT\r\nContent-Length: 1256\r\n\r\n'
    ---- Read response and forward
b'<!doctype html>\n<html>\n<head>\n    <title>Example Domain</title
a charset="utf-8" />\n    <meta http-equiv="Content-type" content="
arset=utf-8" />\n    <meta name="viewport" content="width=device-wi
scale=1" />\n    <style type="text/css">\n    body {\n        backg
#f0f0f2;\n        margin: 0;\n        padding: 0;\n        font-fam
ystem, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "He
 Helvetica, Arial, sans-serif;\n        \n    }\n    div {\n
;\n        margin: 5em auto;\n        padding: 2em;\n        backg
```

[SEED Labs] Capturing from br-55884b75a206
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
45	2024-03-25 19:0…	93.184.216.34	10.9.0.143	TLSv1.3	3776	Server Hello, Applic
46	2024-03-25 19:0…	10.9.0.143	93.184.216.34	TCP	54	40492 → 443 [ACK] Se
47	2024-03-25 19:0…	10.9.0.143	93.184.216.34	TLSv1.3	128	Application Data
48	2024-03-25 19:0…	93.184.216.34	10.9.0.143	TCP	54	443 → 40492 [ACK] Se
49	2024-03-25 19:0…	10.9.0.143	93.184.216.34	TLSv1.3	403	Application Data
50	2024-03-25 19:0…	93.184.216.34	10.9.0.143	TCP	54	443 → 40492 [ACK] Se
51	2024-03-25 19:0…	93.184.216.34	10.9.0.143	TLSv1.3	532	Application Data, Ap
52	2024-03-25 19:0…	10.9.0.143	93.184.216.34	TCP	54	40492 → 443 [ACK] Se
53	2024-03-25 19:0…	93.184.216.34	10.9.0.143	TLSv1.3	1693	Application Data, Ap
54	2024-03-25 19:0…	10.9.0.143	93.184.216.34	TCP	54	40492 → 443 [ACK] Se
55	2024-03-25 19:0…	10.9.0.143	10.9.0.1	TLSv1.3	427	Application Data
56	2024-03-25 19:0…	10.9.0.1	10.9.0.143	TCP	66	51674 → 443 [ACK] Se
57	2024-03-25 19:0…	10.9.0.143	10.9.0.1	TLSv1.3	1344	Application Data
58	2024-03-25 19:0…	10.9.0.1	10.9.0.143	TCP	66	51674 → 443 [ACK] Se
59	2024-03-25 19:0…	10.9.0.1	10.9.0.143	TLSv1.3	382	Application Data
60	2024-03-25 19:0…	10.9.0.143	10.9.0.1	TCP	66	443 → 51674 [ACK] Se
61	2024-03-25 19:0…	02:42:39:cb:32:e4	02:42:0a:09:00:8f	ARP	42	Who has 10.9.0.143?
62	2024-03-25 19:0…	02:42:0a:09:00:8f	02:42:39:cb:32:e4	ARP	42	10.9.0.143 is at 02:
63	2024-03-25 19:0…	10.9.0.1	10.9.0.143	TCP	66	[TCP Keep-Alive] 516
64	2024-03-25 19:0…	10.9.0.143	10.9.0.1	TCP	66	[TCP Keep-Alive ACK]
65	2024-03-25 19:0…	10.9.0.1	10.9.0.143	TCP	66	[TCP Keep-Alive] 516
66	2024-03-25 19:0…	10.9.0.143	10.9.0.1	TCP	66	[TCP Keep-Alive ACK]

```
› Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface br-55884b75a206, id
› Ethernet II, Src: 02:42:39:cb:32:e4 (02:42:39:cb:32:e4), Dst: 02:42:0a:09:00:8f (02:42:0a:09:00:8f)
› Internet Protocol Version 4, Src: 10.9.0.1, Dst: 10.9.0.143
0000  02 42 0a 09 00 8f 02 42  39 cb 32 e4 08 00 45 00   ·B·····B 9·2···E·
```