CDP PMA

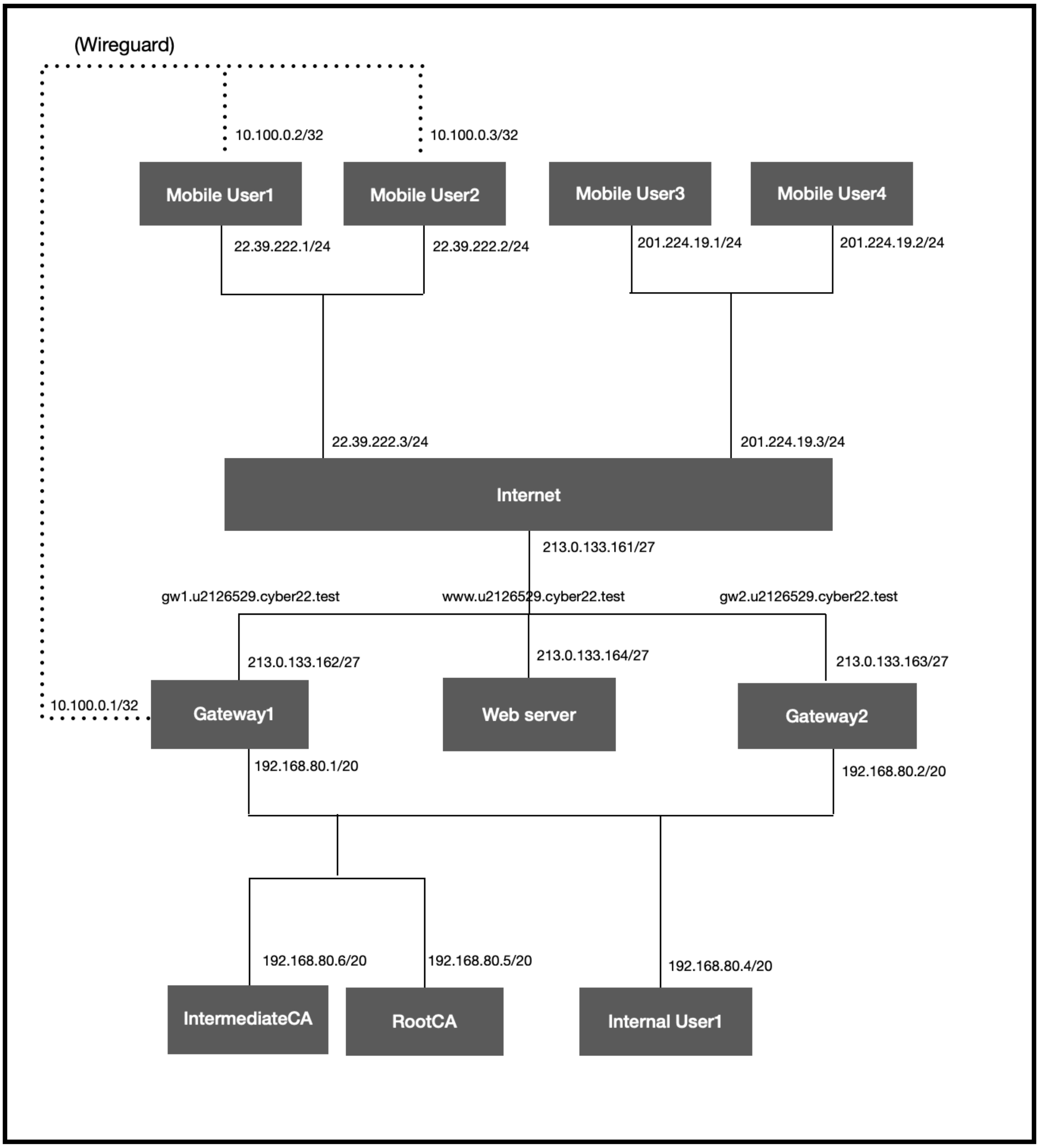
Student ID or IDs for group work	2126529
Module Date	12th - 16th December 2022
GPG Fingerprint	18B0 E637 53AB 5B71 C6F7 3DBE C61F B50D 94D8 BD5B

Date set	16th Dec 2022
Submission date (excluding extensions)	23rd Jan 2023 by 12:00pm (UK time)
Submission guidance	Several files (six) of several types to be submitted electronically via tabula (See Assignment Specification supplied separately) Also viva / demo
Late submission policy	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). “Late” means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late. For **Postgraduate** students only, who started their **current course before 1 August 2019**, the daily penalty is **3 marks** rather than 5.
Resubmission policy	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.

Module title & code	ES94N-15 Cryptosystems and Data Protection (CDP)
Module owner	Peter Norris
Module tutor	Peter Norris
Module marker	Peter Norris
Assessment type	Technical securing of organisation’s assets (design, implement, test) in emulated environment, evaluation of proposal, with demo/viva and challenge response to be returned in the marking window.
Weighting of mark	100%

Phase1:

1.1 Correctly use allocated IP addresses and domain names and show in diagram



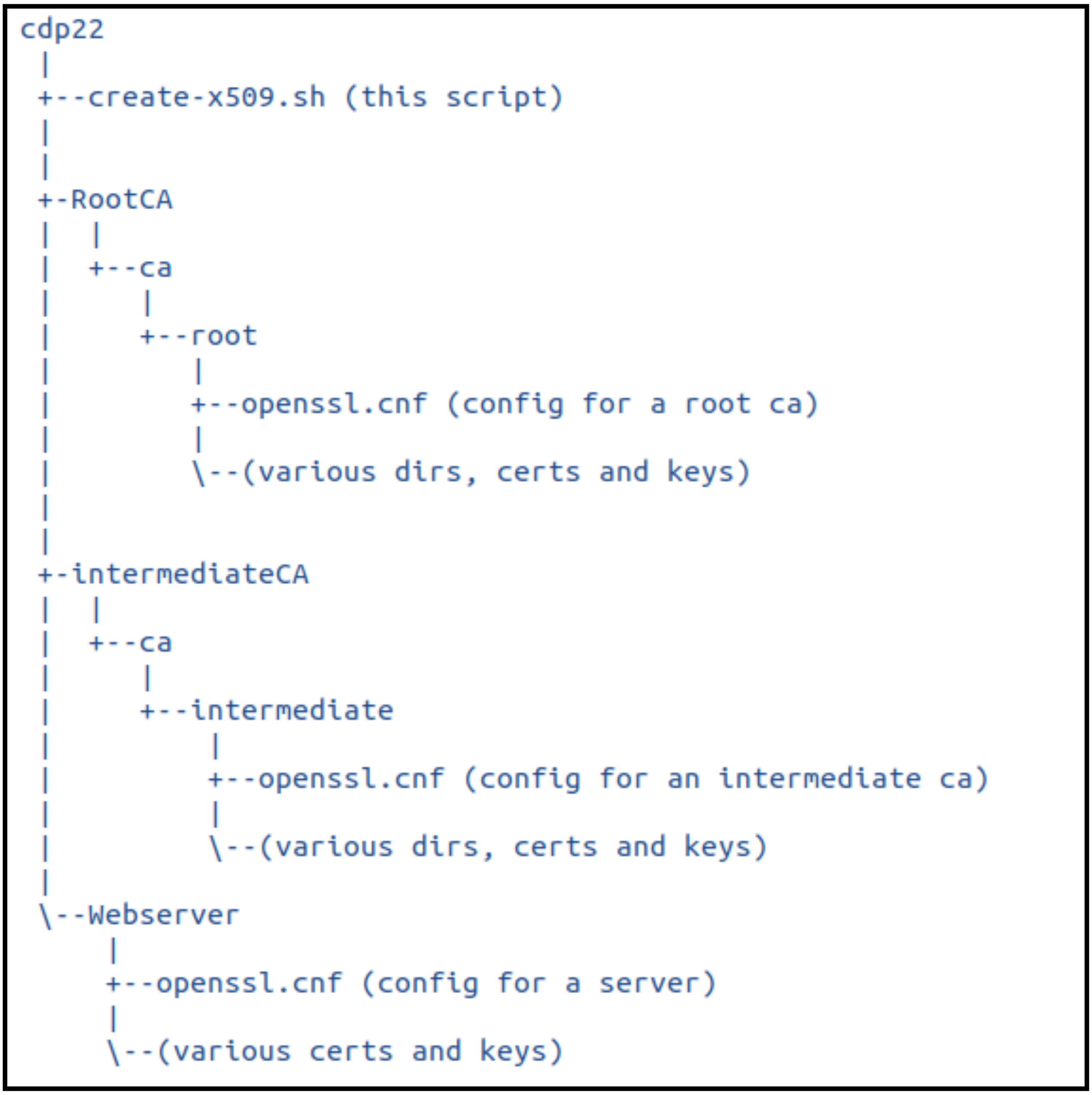
1.2 Correctly use allocated IP addresses and domain names and show in table

Host Name	IP Address
Internal User1	192.168.80.4/20
Root CA	192.168.80.5/20
Intermediate CA	192.168.80.6/20
Gateway1	192.168.80.1/20, 213.0.133.162/27, (10.100.0.1/32)
Gateway2	192.168.80.2/20, 213.0.133.163/27
Web server	213.0.133.164/27
Internet	213.0.133.161/27, 22.39.222.3/24, 201.224.19.3/24
Mobile User1	22.39.222.1/24, (10.100.0.2/32)
Mobile User2	22.39.222.2/24, (10.100.0.3/32)
Mobile User3	201.224.19.1/24
Mobile User4	201.224.19.2/24

Host Name	IP Address	Domain Name
Gateway1	213.0.133.162/27	gw1.u2126529.cyber22.test
Gateway2	213.0.133.163/27	gw2.u2126529.cyber22.test
Web server	213.0.133.164/27	www.u2126529.cyber22.test

1.3 Define and implement a credible x509 certificate hierarchy for the organisation, consistent with the script of instructions used to achieve this[2]

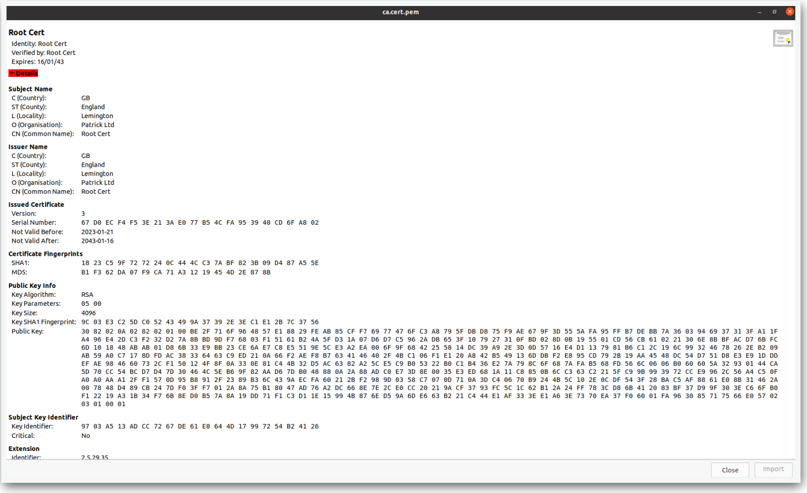
1.3.1 Certificate hierarchy: Root - Intermediate - Server



```
cdp22
 |
 +--create-x509.sh (this script)
 |
 |
 +-RootCA
 |  |
 |  +--ca
 |     |
 |     +--root
 |        |
 |        +--openssl.cnf (config for a root ca)
 |        |
 |        \--(various dirs, certs and keys)
 |
 |
 +-intermediateCA
 |  |
 |  +--ca
 |     |
 |     +--intermediate
 |         |
 |         +--openssl.cnf (config for an intermediate ca)
 |         |
 |         \--(various dirs, certs and keys)
 |
 \--Webserver
     |
     +--openssl.cnf (config for a server)
     |
     \--(various certs and keys)
```

1.3.2 Show the evidences of certificates

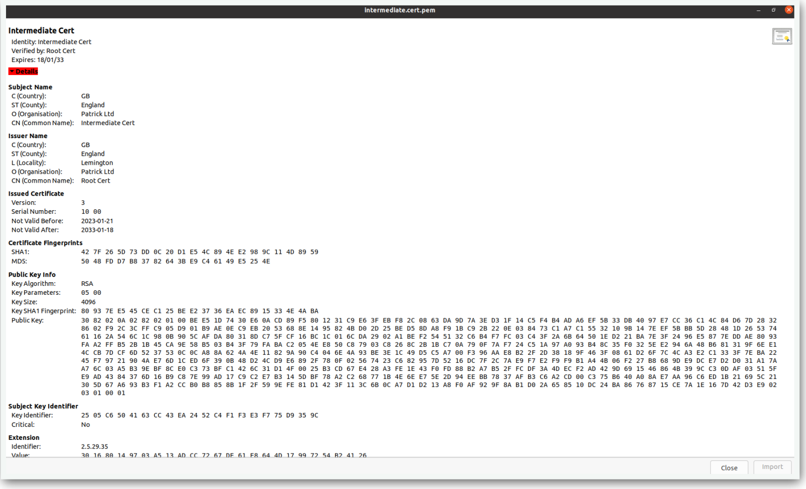
- Root cert (RootCA/ca/root/certs/ca.cert.pem):



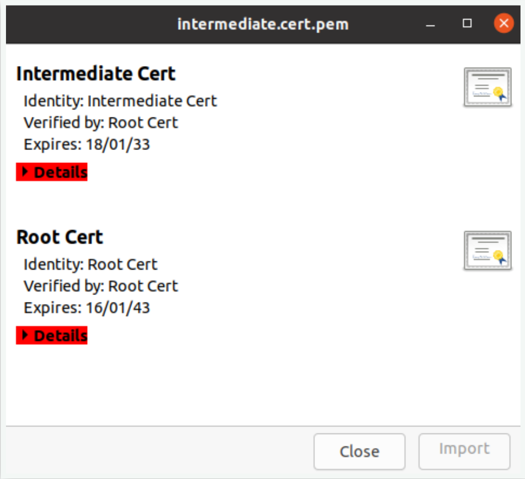
```
Root Cert
  Identity: Root Cert
  Verified by: Root Cert
  Expires: 16/01/43
▾ Details

Subject Name
  C (Country):           GB
  ST (County):           England
  L (Locality):          Lemington
  O (Organisation):      Patrick Ltd
  CN (Common Name):      Root Cert
Issuer Name
  C (Country):           GB
  ST (County):           England
  L (Locality):          Lemington
  O (Organisation):      Patrick Ltd
  CN (Common Name):      Root Cert
Issued Certificate
  Version:               3
  Serial Number:         67 D0 EC F4 F5 3E 21 3A E0 77 B5 4C FA 95 39 40 CD 6F A8 02
  Not Valid Before:      2023-01-21
  Not Valid After:       2043-01-16
Certificate Fingerprints
  SHA1:                  18 23 C5 9F 72 72 24 0C 44 4C C3 7A BF 82 3B 09 D4 87 A5 5E
  MD5:                   B1 F3 62 DA 07 F9 CA 71 A3 12 19 45 4D 2E 87 8B
Public Key Info
  Key Algorithm:         RSA
  Key Parameters:        05 00
  Key Size:              4096
  Key SHA1 Fingerprint:  9C 03 E3 C2 5D C0 52 43 49 9A 37 39 2E 3E C1 E1 2B 7C 37 56
  Public Key:            30 82 02 0A 02 82 02 01 00 BE 2F 71 6F 96 48 57 E1 88 29 FE AB 85 CF F7 69 77 47 6F C3 A8 79 5F DB D8 75 F9 AE 67 9F 3D 55 5A FA 95 FF B7 DE BB 7A 36 03 94 69 37 31 3F A1 1F
                         A4 96 E4 2D C3 F2 32 D2 7A 8B BD 9D F7 68 03 F1 51 61 B2 4A 5F D3 1A 07 D6 D7 C5 96 2A DB 65 3F 10 79 27 31 0F BD 02 8D 0B 19 55 01 CD 56 CB 61 02 21 30 6E 8B BF AC D7 6B FC
                         6D 10 18 48 AB AB 01 D8 6B 33 E9 BB 23 CE 6A E7 C8 E5 51 9E 5C E3 A2 EA 00 6F 9F 68 42 25 58 14 DC 39 A9 2E 3D 0D 57 16 E4 D1 13 79 81 B6 C1 2C 19 6C 99 32 46 78 26 2E B2 09
                         AB 59 A0 C7 17 8D FD AC 38 33 64 63 C9 ED 21 0A 66 F2 AE F8 B7 63 41 46 40 2F 4B C1 06 F1 E1 20 A8 42 B5 49 13 6D DB F2 E8 95 CD 79 2B 19 AA 45 48 DC 54 D7 51 D8 E3 E9 1D DD
                         EF AE 98 46 60 73 2C F1 50 12 4F 8F 0A 33 0E 81 C4 4B 32 D5 AC 63 82 A2 5C E5 C9 B0 53 22 B0 C1 B4 36 E2 7A 79 8C 6F 68 7A FA B5 68 FD 56 6C 06 06 B0 60 60 5A 32 93 01 44 CA
                         5D 70 CC 54 BC D7 D4 7D 30 46 4C 5E B6 9F 82 AA D6 7D B0 48 88 0A 2A 88 AD C0 E7 3D 8E 00 35 E3 ED 68 1A 11 C8 85 0B 6C C3 63 C2 21 5F C9 9B 99 39 72 CC E9 96 2C 56 A4 C5 0F
                         A0 A0 AA A1 2F F1 57 0D 95 B8 91 2F 23 89 B3 6C 43 9A EC FA 60 21 2B F2 98 9D 03 58 C7 07 0D 71 0A 3D C4 06 70 B9 24 4B 5C 10 2E 0C DF 54 3F 28 BA C5 AF 88 61 E0 8B 31 46 2A
                         00 78 48 D4 89 CB 24 7D F0 3F F7 01 2A 8A 75 B1 80 47 AD 76 A2 DC 66 8E 7E 2C E0 CC 20 21 9A CF 37 93 FC 5C 1C 62 B1 2A 24 FF 78 3C D8 6B 41 20 83 BF 37 D9 9F 30 3E C6 6F B0
                         F1 22 19 A3 1B 34 F7 6B 8E D0 B5 7A 8A 19 DD 71 F1 C3 D1 1E 15 99 4B 87 6E D5 9A 6D E6 63 B2 21 C4 44 E1 AF 33 3E E1 A6 3E 73 70 EA 37 F0 60 01 FA 96 30 85 71 75 66 E0 57 02
                         03 01 00 01
Subject Key Identifier
  Key Identifier:        97 03 A5 13 AD CC 72 67 DE 61 E8 64 4D 17 99 72 54 B2 41 26
  Critical:              No
Extension
  Identifier:            2.5.29.35
```

- Intermediate cert and CA Chain (IntermediateCA/ca/root/certs/Intermediate.cert.pem):

We use CA chain to verity server cert by intermediate cert

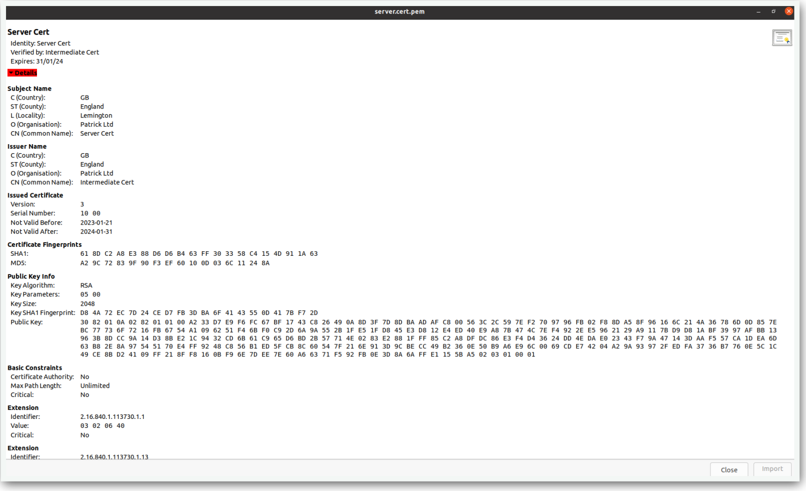


```
Intermediate Cert
  Identity: Intermediate Cert
  Verified by: Root Cert
  Expires: 18/01/33
▾ Details

Subject Name
  C (Country):           GB
  ST (County):           England
  O (Organisation):      Patrick Ltd
  CN (Common Name):      Intermediate Cert
Issuer Name
  C (Country):           GB
  ST (County):           England
  L (Locality):          Lemington
  O (Organisation):      Patrick Ltd
  CN (Common Name):      Root Cert
Issued Certificate
  Version:               3
  Serial Number:         10 00
  Not Valid Before:      2023-01-21
  Not Valid After:       2033-01-18
Certificate Fingerprints
  SHA1:                  42 7F 26 5D 73 DD 0C 20 D1 E5 4C 89 4E E2 98 9C 11 4D 89 59
  MD5:                   50 48 FD D7 B8 37 82 64 3B E9 C4 61 49 E5 25 4E
Public Key Info
  Key Algorithm:         RSA
  Key Parameters:        05 00
  Key Size:              4096
  Key SHA1 Fingerprint:  80 93 7E E5 45 CE C1 25 BE E2 37 36 EA EC 89 15 33 4E 4A BA
  Public Key:            30 82 02 0A 02 82 02 01 00 BE E5 1D 74 30 E6 0A CD 89 F5 80 12 31 C9 E6 3F EB F8 2C 08 63 DA 9D 7A 3E D3 1F 14 C5 F4 B4 AD A6 EF 5B 33 DB 40 97 E7 CC 36 C1 4C 84 D6 7D 28 32
                         86 02 F9 2C 3C FF C9 05 D9 01 B9 AE 0E C9 EB 20 53 68 8E 14 95 82 4B D0 2D 25 BE D5 8D A8 F9 1B C9 2B 22 0E 03 84 73 C1 A7 C1 55 32 10 9B 14 7E EF 5B BB 5D 28 48 1D 26 53 74
                         61 16 2A 54 6C 1C 98 0B 90 5C AF DA 80 31 8D C7 5F CF 16 BC 1C 01 6C DA 29 02 A1 BE F2 54 51 32 C6 B4 F7 FC 03 C4 3F 2A 6B 64 50 1E D2 21 BA 7E 3F 24 96 E5 87 7E DD AE 80 93
                         FA A2 FF B5 2B 1B 45 CA 9E 58 B5 03 B4 3F 79 FA BA C2 05 4E E8 50 C8 79 03 C8 26 8C 2B 1B C7 0A 79 0F 7A F7 24 C5 1A 97 A0 93 B4 8C 35 F0 32 5E E2 94 6A 48 B6 81 31 9F 6E E1
                         4C CB 7D CF 6D 52 37 53 0C 0C A8 8A 62 4A 4E 11 82 9A 90 C4 04 6E 4A 93 BE 3E 1C 49 D5 C5 A7 00 F3 96 AA E8 B2 2F 2D 38 18 9F 46 3F 08 61 D2 6F 7C 4C A3 E2 C1 33 3F 7E BA 22
                         45 F7 97 21 90 4A E7 6D 1C ED 6F 39 0B 48 D2 4C D9 E6 89 2F 78 0F 02 56 74 23 C6 82 95 7D 52 16 DC 7F 2C 7A E9 F7 E2 F9 F9 B1 A4 4B 06 F2 27 B8 68 9D E9 DC E7 D2 D0 31 A1 7A
                         A7 6C 03 A5 B3 9E BF 8C E0 C3 73 BF C1 42 6C 31 D1 4F 00 25 B3 CD 67 E4 28 A3 FE 1E 43 F0 FD 88 B2 A7 B5 2F FC DF 3A 4D EC F2 AD 42 9D 69 15 46 86 4B 39 9C C3 0D AF 03 51 5F
                         E9 AD 43 84 37 6D 16 B9 C8 7E 99 AD 17 C9 C2 E7 B3 14 5D BF 78 A2 C2 68 77 1B 4E 6E E7 5E 2D 94 EE BB 78 37 AF B3 C6 A2 CD 00 C3 75 B6 40 A0 8A E7 AA 96 C6 ED 1B 21 69 5C 21
                         30 5D 67 A6 93 B3 F1 A2 CC B0 B8 85 8B 1F 2F 59 9E FE 81 D1 42 3F 11 3C 6B 0C A7 D1 D2 13 A8 F0 AF 92 9F 8A B1 D0 2A 65 85 10 DC 24 BA 86 76 87 15 CE 7A 1E 16 7D 42 D3 E9 02
                         03 01 00 01
Subject Key Identifier
  Key Identifier:        25 05 C6 50 41 63 CC 43 EA 24 52 C4 F1 F3 E3 F7 75 D9 35 9C
  Critical:              No
Extension
  Identifier:            2.5.29.35
  Value:                 30 16 80 14 97 03 A5 13 AD CC 72 67 DE 61 E8 64 4D 17 99 72 54 B2 41 26
```



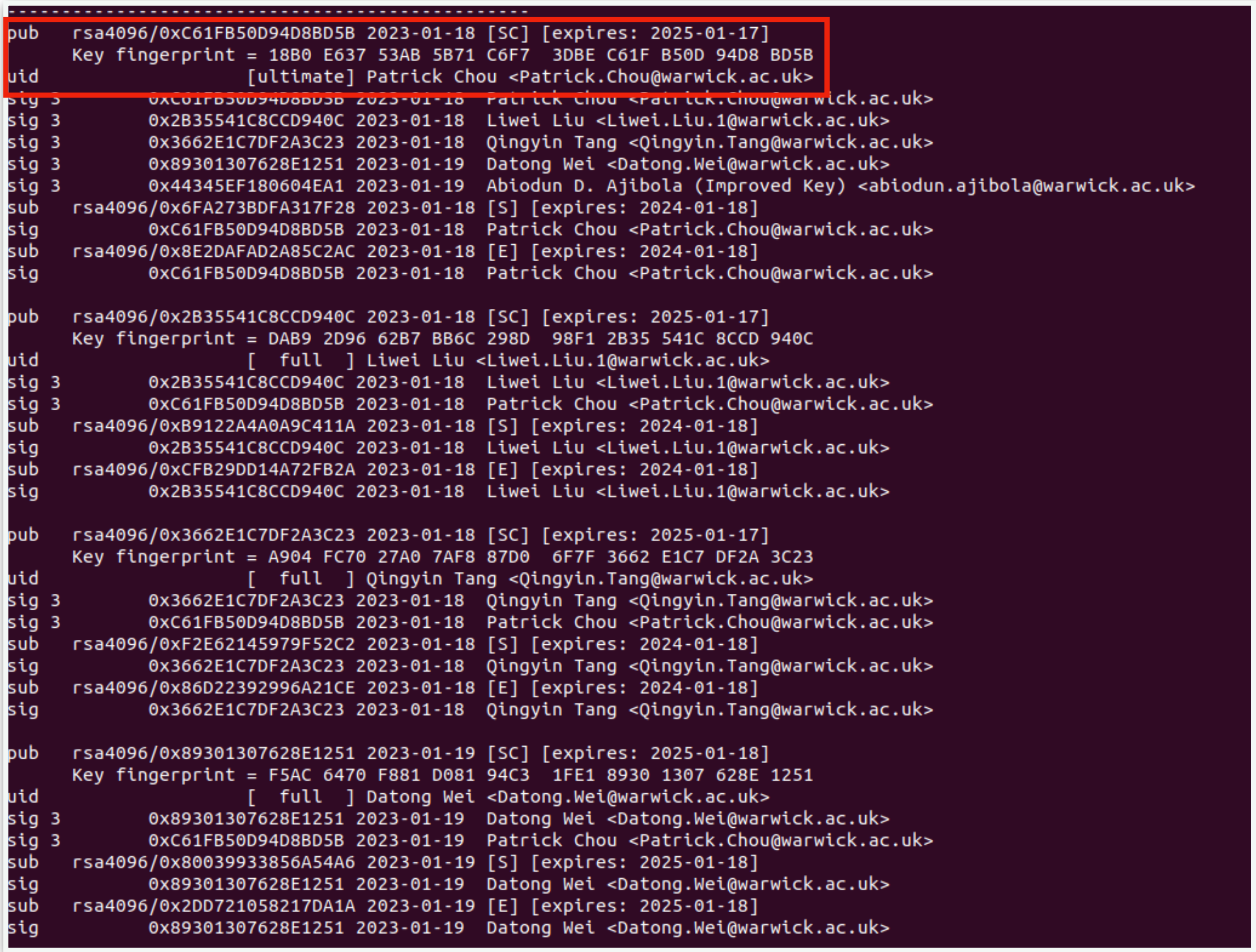
```
Intermediate Cert
  Identity: Intermediate Cert
  Verified by: Root Cert
  Expires: 18/01/33
▸ Details

Root Cert
  Identity: Root Cert
  Verified by: Root Cert
  Expires: 16/01/43
▸ Details
```

- Server cert (Webserver/server.cert.pem):



```
Server Cert
  Identity: Server Cert
  Verified by: Intermediate Cert
  Expires: 31/01/24
▾ Details

Subject Name
  C (Country):           GB
  ST (County):           England
  L (Locality):          Lemington
  O (Organisation):      Patrick Ltd
  CN (Common Name):      Server Cert
Issuer Name
  C (Country):           GB
  ST (County):           England
  O (Organisation):      Patrick Ltd
  CN (Common Name):      Intermediate Cert
Issued Certificate
  Version:               3
  Serial Number:         10 00
  Not Valid Before:      2023-01-21
  Not Valid After:       2024-01-31
Certificate Fingerprints
  SHA1:                  61 8D C2 A8 E3 88 D6 D6 B4 63 FF 30 33 58 C4 15 4D 91 1A 63
  MD5:                   A2 9C 72 83 9F 90 F3 EF 60 10 0D 03 6C 11 24 8A
Public Key Info
  Key Algorithm:         RSA
  Key Parameters:        05 00
  Key Size:              2048
  Key SHA1 Fingerprint:  D8 4A 72 EC 7D 24 CE D7 FB 3D BA 6F 41 43 55 0D 41 7B F7 2D
  Public Key:            30 82 01 0A 02 82 01 01 00 A2 33 D7 E9 F6 FC 67 BF 17 43 C8 26 49 0A 8D 3F 7D 8D BA AD AF C8 00 56 3C 2C 59 7E F2 70 97 96 FB 02 F8 8D A5 8F 96 16 6C 21 4A 36 78 6D 0D 85 7E
                         BC 77 73 6F 72 16 FB 67 54 A1 09 62 51 F4 6B F0 C9 2D 6A 9A 55 2B 1F E5 1F D8 45 E3 D8 12 E4 ED 40 E9 A8 7B 47 4C 7E F4 92 2E E5 96 21 29 A9 11 7B D9 D8 1A BF 39 97 AF BB 13
                         96 3B 8D CC 9A 14 D3 8B E2 1C 94 32 CD 6B 61 C9 65 D6 BD 2B 57 71 4E 02 83 E2 88 1F FF 85 C2 A8 DF DC 86 E3 F4 D4 36 24 DD 4E DA E0 23 43 F7 9A 47 14 3D AA F5 57 CA 1D EA 6D
                         63 B8 2E 8A 97 54 51 70 E4 FF 92 48 C8 56 B1 ED 5F CB 8C 60 54 7F 21 6E 91 3D 9C BE CC 49 B2 36 0E 50 B9 A6 E9 6C 00 69 CD E7 42 04 A2 9A 93 97 2F ED FA 37 36 B7 76 0E 5C 1C
                         49 CE 8B D2 41 09 FF 21 8F F8 16 0B F9 6E 7D EE 7E 60 A6 63 71 F5 92 FB 0E 3D 8A 6A FF E1 15 5B A5 02 03 01 00 01
Basic Constraints
  Certificate Authority: No
  Max Path Length:       Unlimited
  Critical:              No
Extension
  Identifier:            2.16.840.1.113730.1.1
  Value:                 03 02 06 40
  Critical:              No
Extension
  Identifier:            2.16.840.1.113730.1.13
```

1.4 Submit a GPG public key that is consistent with your University of Warwick email and valid until at least November 2024[1]



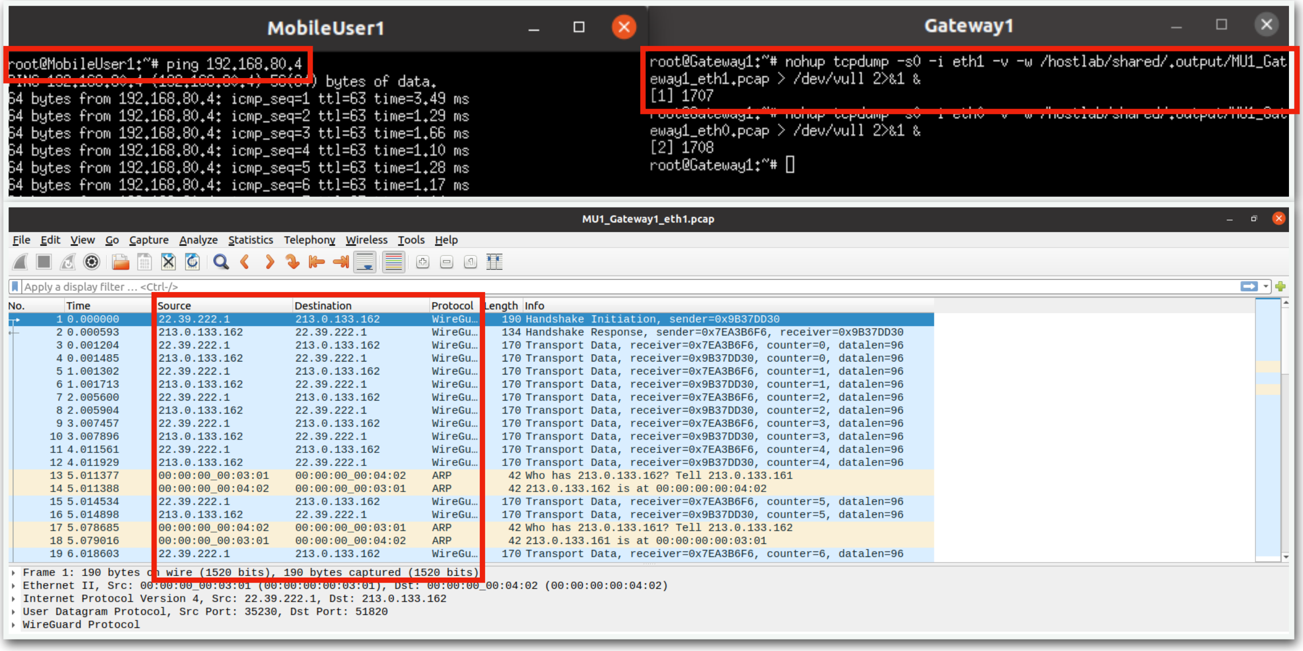
```
-------------------------------------------------
pub   rsa4096/0xC61FB50D94D8BD5B 2023-01-18 [SC] [expires: 2025-01-17]
      Key fingerprint = 18B0 E637 53AB 5B71 C6F7  3DBE C61F B50D 94D8 BD5B
uid                 [ultimate] Patrick Chou <Patrick.Chou@warwick.ac.uk>
sig 3        0xC61FB50D94D8BD5B 2023-01-18  Patrick Chou <Patrick.Chou@warwick.ac.uk>
sig 3        0x2B35541C8CCD940C 2023-01-18  Liwei Liu <Liwei.Liu.1@warwick.ac.uk>
sig 3        0x3662E1C7DF2A3C23 2023-01-18  Qingyin Tang <Qingyin.Tang@warwick.ac.uk>
sig 3        0x89301307628E1251 2023-01-19  Datong Wei <Datong.Wei@warwick.ac.uk>
sig 3        0x44345EF180604EA1 2023-01-19  Abiodun D. Ajibola (Improved Key) <abiodun.ajibola@warwick.ac.uk>
sub   rsa4096/0x6FA273BDFA317F28 2023-01-18 [S] [expires: 2024-01-18]
sig          0xC61FB50D94D8BD5B 2023-01-18  Patrick Chou <Patrick.Chou@warwick.ac.uk>
sub   rsa4096/0x8E2DAFAD2A85C2AC 2023-01-18 [E] [expires: 2024-01-18]
sig          0xC61FB50D94D8BD5B 2023-01-18  Patrick Chou <Patrick.Chou@warwick.ac.uk>

pub   rsa4096/0x2B35541C8CCD940C 2023-01-18 [SC] [expires: 2025-01-17]
      Key fingerprint = DAB9 2D96 62B7 BB6C 298D  98F1 2B35 541C 8CCD 940C
uid                 [  full  ] Liwei Liu <Liwei.Liu.1@warwick.ac.uk>
sig 3        0x2B35541C8CCD940C 2023-01-18  Liwei Liu <Liwei.Liu.1@warwick.ac.uk>
sig 3        0xC61FB50D94D8BD5B 2023-01-18  Patrick Chou <Patrick.Chou@warwick.ac.uk>
sub   rsa4096/0xB9122A4A0A9C411A 2023-01-18 [S] [expires: 2024-01-18]
sig          0x2B35541C8CCD940C 2023-01-18  Liwei Liu <Liwei.Liu.1@warwick.ac.uk>
sub   rsa4096/0xCFB29DD14A72FB2A 2023-01-18 [E] [expires: 2024-01-18]
sig          0x2B35541C8CCD940C 2023-01-18  Liwei Liu <Liwei.Liu.1@warwick.ac.uk>

pub   rsa4096/0x3662E1C7DF2A3C23 2023-01-18 [SC] [expires: 2025-01-17]
      Key fingerprint = A904 FC70 27A0 7AF8 87D0  6F7F 3662 E1C7 DF2A 3C23
uid                 [  full  ] Qingyin Tang <Qingyin.Tang@warwick.ac.uk>
sig 3        0x3662E1C7DF2A3C23 2023-01-18  Qingyin Tang <Qingyin.Tang@warwick.ac.uk>
sig 3        0xC61FB50D94D8BD5B 2023-01-18  Patrick Chou <Patrick.Chou@warwick.ac.uk>
sub   rsa4096/0xF2E62145979F52C2 2023-01-18 [S] [expires: 2024-01-18]
sig          0x3662E1C7DF2A3C23 2023-01-18  Qingyin Tang <Qingyin.Tang@warwick.ac.uk>
sub   rsa4096/0x86D22392996A21CE 2023-01-18 [E] [expires: 2024-01-18]
sig          0x3662E1C7DF2A3C23 2023-01-18  Qingyin Tang <Qingyin.Tang@warwick.ac.uk>

pub   rsa4096/0x89301307628E1251 2023-01-19 [SC] [expires: 2025-01-18]
      Key fingerprint = F5AC 6470 F881 D081 94C3  1FE1 8930 1307 628E 1251
uid                 [  full  ] Datong Wei <Datong.Wei@warwick.ac.uk>
sig 3        0x89301307628E1251 2023-01-19  Datong Wei <Datong.Wei@warwick.ac.uk>
sig 3        0xC61FB50D94D8BD5B 2023-01-19  Patrick Chou <Patrick.Chou@warwick.ac.uk>
sub   rsa4096/0x80039933856A54A6 2023-01-19 [S] [expires: 2025-01-18]
sig          0x89301307628E1251 2023-01-19  Datong Wei <Datong.Wei@warwick.ac.uk>
sub   rsa4096/0x2DD721058217DA1A 2023-01-19 [E] [expires: 2025-01-18]
sig          0x89301307628E1251 2023-01-19  Datong Wei <Datong.Wei@warwick.ac.uk>
```

1.5 Achieve VPN connectivity for at least two sample mobile workers over WireGuard, and have evidence that the VPN functions correctly[3]

1.5.1 MobileUser1-Wireguard

We use ping from MobileUser1 (22.39.222.1/24) to InternalUser1(192.168.80.4/20) and use tcpdump to catch the packets on eth0 (192.168.80.1/20) and eth1 (213.0.133.162/27) of Gateway1

- MobileUser1-Wireguard-eth1 (/hostlab/shared/.output/MU1_Gateway1_eth1.pcap)

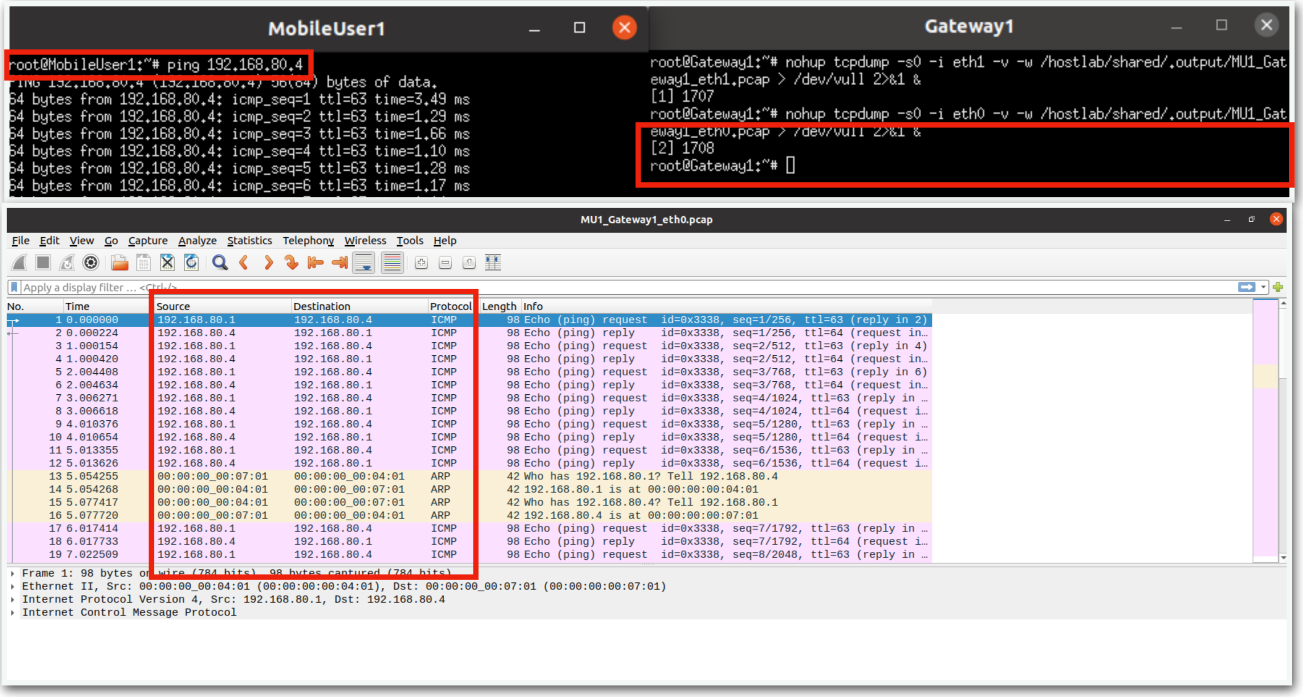

MobileUser1
Gateway1
MU1_Gateway1_eth1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
root@MobileUser1:~# ping 192.168.80.4
PING 192.168.80.4 (192.168.80.4) 56(84) bytes of data.
64 bytes from 192.168.80.4: icmp_seq=1 ttl=63 time=3.49 ms
64 bytes from 192.168.80.4: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 192.168.80.4: icmp_seq=3 ttl=63 time=1.66 ms
64 bytes from 192.168.80.4: icmp_seq=4 ttl=63 time=1.10 ms
64 bytes from 192.168.80.4: icmp_seq=5 ttl=63 time=1.28 ms
64 bytes from 192.168.80.4: icmp_seq=6 ttl=63 time=1.17 ms
```

```
root@Gateway1:~# nohup tcpdump -s0 -i eth1 -v -w /hostlab/shared/.output/MU1_Gat
eway1_eth1.pcap > /dev/vull 2>&1 &
[1] 1707
root@Gateway1:~# nohup tcpdump -s0 -i eth0 -v -w /hostlab/shared/.output/MU1_Gat
eway1_eth0.pcap > /dev/vull 2>&1 &
[2] 1708
root@Gateway1:~# 
```

```
No.   Time       Source              Destination         Protocol Length Info
    1 0.000000   22.39.222.1         213.0.133.162       WireGu…   190 Handshake Initiation, sender=0x9B37DD30
    2 0.000593   213.0.133.162       22.39.222.1         WireGu…   134 Handshake Response, sender=0x7EA3B6F6, receiver=0x9B37DD30
    3 0.001204   22.39.222.1         213.0.133.162       WireGu…   170 Transport Data, receiver=0x7EA3B6F6, counter=0, datalen=96
    4 0.001485   213.0.133.162       22.39.222.1         WireGu…   170 Transport Data, receiver=0x9B37DD30, counter=0, datalen=96
    5 1.001302   22.39.222.1         213.0.133.162       WireGu…   170 Transport Data, receiver=0x7EA3B6F6, counter=1, datalen=96
    6 1.001713   213.0.133.162       22.39.222.1         WireGu…   170 Transport Data, receiver=0x9B37DD30, counter=1, datalen=96
    7 2.005600   22.39.222.1         213.0.133.162       WireGu…   170 Transport Data, receiver=0x7EA3B6F6, counter=2, datalen=96
    8 2.005904   213.0.133.162       22.39.222.1         WireGu…   170 Transport Data, receiver=0x9B37DD30, counter=2, datalen=96
    9 3.007457   22.39.222.1         213.0.133.162       WireGu…   170 Transport Data, receiver=0x7EA3B6F6, counter=3, datalen=96
   10 3.007896   213.0.133.162       22.39.222.1         WireGu…   170 Transport Data, receiver=0x9B37DD30, counter=3, datalen=96
   11 4.011561   22.39.222.1         213.0.133.162       WireGu…   170 Transport Data, receiver=0x7EA3B6F6, counter=4, datalen=96
   12 4.011929   213.0.133.162       22.39.222.1         WireGu…   170 Transport Data, receiver=0x9B37DD30, counter=4, datalen=96
   13 5.011377   00:00:00_00:03:01   00:00:00_00:04:02   ARP        42 Who has 213.0.133.162? Tell 213.0.133.161
   14 5.011388   00:00:00_00:04:02   00:00:00_00:03:01   ARP        42 213.0.133.162 is at 00:00:00:00:04:02
   15 5.014534   22.39.222.1         213.0.133.162       WireGu…   170 Transport Data, receiver=0x7EA3B6F6, counter=5, datalen=96
   16 5.014898   213.0.133.162       22.39.222.1         WireGu…   170 Transport Data, receiver=0x9B37DD30, counter=5, datalen=96
   17 5.078685   00:00:00_00:04:02   00:00:00_00:03:01   ARP        42 Who has 213.0.133.161? Tell 213.0.133.162
   18 5.079016   00:00:00_00:03:01   00:00:00_00:04:02   ARP        42 213.0.133.161 is at 00:00:00:00:03:01
   19 6.018603   22.39.222.1         213.0.133.162       WireGu…   170 Transport Data, receiver=0x7EA3B6F6, counter=6, datalen=96

› Frame 1: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits)
› Ethernet II, Src: 00:00:00_00:03:01 (00:00:00:00:03:01), Dst: 00:00:00_00:04:02 (00:00:00:00:04:02)
› Internet Protocol Version 4, Src: 22.39.222.1, Dst: 213.0.133.162
› User Datagram Protocol, Src Port: 35230, Dst Port: 51820
› WireGuard Protocol
```

- MobileUser1-Wireguard-eth0 (/hostlab/shared/.output/MU1_Gateway1_eth0.pcap)


MobileUser1
Gateway1
MU1_Gateway1_eth0.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
root@MobileUser1:~# ping 192.168.80.4
PING 192.168.80.4 (192.168.80.4) 56(84) bytes of data.
64 bytes from 192.168.80.4: icmp_seq=1 ttl=63 time=3.49 ms
64 bytes from 192.168.80.4: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 192.168.80.4: icmp_seq=3 ttl=63 time=1.66 ms
64 bytes from 192.168.80.4: icmp_seq=4 ttl=63 time=1.10 ms
64 bytes from 192.168.80.4: icmp_seq=5 ttl=63 time=1.28 ms
64 bytes from 192.168.80.4: icmp_seq=6 ttl=63 time=1.17 ms
```

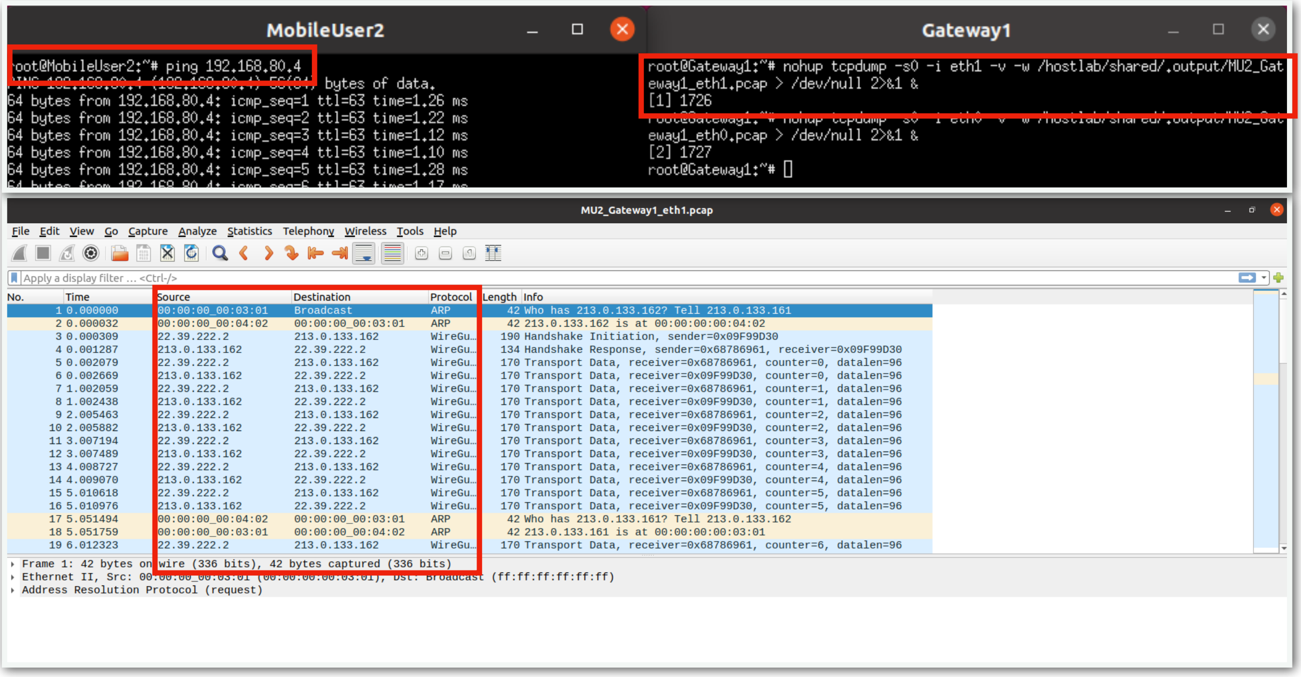
```
root@Gateway1:~# nohup tcpdump -s0 -i eth1 -v -w /hostlab/shared/.output/MU1_Gat
eway1_eth1.pcap > /dev/vull 2>&1 &
[1] 1707
root@Gateway1:~# nohup tcpdump -s0 -i eth0 -v -w /hostlab/shared/.output/MU1_Gat
eway1_eth0.pcap > /dev/vull 2>&1 &
[2] 1708
root@Gateway1:~# 
```

```
No.   Time       Source              Destination         Protocol Length Info
    1 0.000000   192.168.80.1        192.168.80.4        ICMP       98 Echo (ping) request  id=0x3338, seq=1/256, ttl=63 (reply in 2)
    2 0.000224   192.168.80.4        192.168.80.1        ICMP       98 Echo (ping) reply    id=0x3338, seq=1/256, ttl=64 (request in…
    3 1.000154   192.168.80.1        192.168.80.4        ICMP       98 Echo (ping) request  id=0x3338, seq=2/512, ttl=63 (reply in 4)
    4 1.000420   192.168.80.4        192.168.80.1        ICMP       98 Echo (ping) reply    id=0x3338, seq=2/512, ttl=64 (request in…
    5 2.004408   192.168.80.1        192.168.80.4        ICMP       98 Echo (ping) request  id=0x3338, seq=3/768, ttl=63 (reply in 6)
    6 2.004634   192.168.80.4        192.168.80.1        ICMP       98 Echo (ping) reply    id=0x3338, seq=3/768, ttl=64 (request in…
    7 3.006271   192.168.80.1        192.168.80.4        ICMP       98 Echo (ping) request  id=0x3338, seq=4/1024, ttl=63 (reply in …
    8 3.006618   192.168.80.4        192.168.80.1        ICMP       98 Echo (ping) reply    id=0x3338, seq=4/1024, ttl=64 (request i…
    9 4.010376   192.168.80.1        192.168.80.4        ICMP       98 Echo (ping) request  id=0x3338, seq=5/1280, ttl=63 (reply in …
   10 4.010654   192.168.80.4        192.168.80.1        ICMP       98 Echo (ping) reply    id=0x3338, seq=5/1280, ttl=64 (request i…
   11 5.013355   192.168.80.1        192.168.80.4        ICMP       98 Echo (ping) request  id=0x3338, seq=6/1536, ttl=63 (reply in …
   12 5.013626   192.168.80.4        192.168.80.1        ICMP       98 Echo (ping) reply    id=0x3338, seq=6/1536, ttl=64 (request i…
   13 5.054255   00:00:00_00:07:01   00:00:00_00:04:01   ARP        42 Who has 192.168.80.1? Tell 192.168.80.4
   14 5.054268   00:00:00_00:04:01   00:00:00_00:07:01   ARP        42 192.168.80.1 is at 00:00:00:00:04:01
   15 5.077417   00:00:00_00:04:01   00:00:00_00:07:01   ARP        42 Who has 192.168.80.4? Tell 192.168.80.1
   16 5.077720   00:00:00_00:07:01   00:00:00_00:04:01   ARP        42 192.168.80.4 is at 00:00:00:00:07:01
   17 6.017414   192.168.80.1        192.168.80.4        ICMP       98 Echo (ping) request  id=0x3338, seq=7/1792, ttl=63 (reply in …
   18 6.017733   192.168.80.4        192.168.80.1        ICMP       98 Echo (ping) reply    id=0x3338, seq=7/1792, ttl=64 (request i…
   19 7.022509   192.168.80.1        192.168.80.4        ICMP       98 Echo (ping) request  id=0x3338, seq=8/2048, ttl=63 (reply in …

› Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
› Ethernet II, Src: 00:00:00_00:04:01 (00:00:00:00:04:01), Dst: 00:00:00_00:07:01 (00:00:00:00:07:01)
› Internet Protocol Version 4, Src: 192.168.80.1, Dst: 192.168.80.4
› Internet Control Message Protocol
```

1.5.2 MobileUser2-Wireguard

We use ping from MobileUser2 (22.39.222.2/24) to InternalUser1 (192.168.80.4/20) and use tcpdump to catch the packets on eth0 (192.168.80.1/20) and eth1 (213.0.133.162/27) of Gateway1

- MobileUser2-Wireguard-eth0 (/hostlab/shared/.output/MU2_Gateway1_eth0.pcap)



MobileUser2

```
root@MobileUser2:~# ping 192.168.80.4
PING 192.168.80.4 (192.168.80.4) 56(84) bytes of data.
64 bytes from 192.168.80.4: icmp_seq=1 ttl=63 time=1.26 ms
64 bytes from 192.168.80.4: icmp_seq=2 ttl=63 time=1.22 ms
64 bytes from 192.168.80.4: icmp_seq=3 ttl=63 time=1.12 ms
64 bytes from 192.168.80.4: icmp_seq=4 ttl=63 time=1.10 ms
64 bytes from 192.168.80.4: icmp_seq=5 ttl=63 time=1.28 ms
64 bytes from 192.168.80.4: icmp_seq=6 ttl=63 time=1.17 ms
```

Gateway1

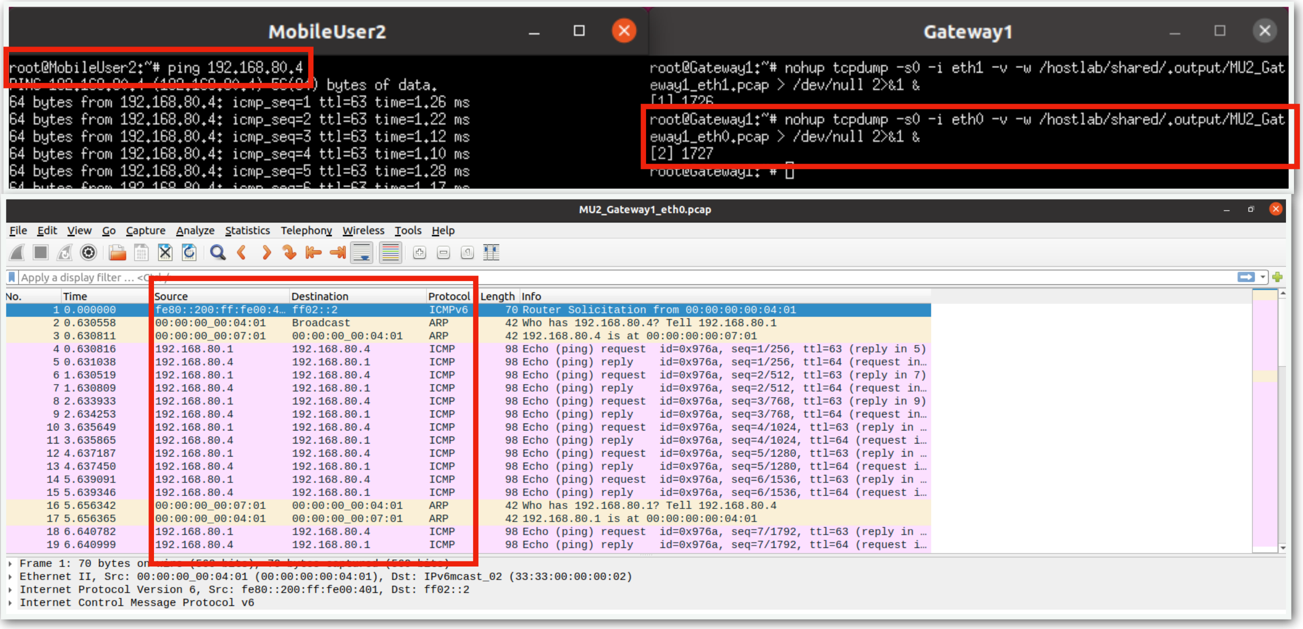
```
root@Gateway1:~# nohup tcpdump -s0 -i eth1 -v -w /hostlab/shared/.output/MU2_Gat
eway1_eth1.pcap > /dev/null 2>&1 &
[1] 1726
root@Gateway1:~# nohup tcpdump -s0 -i eth0 -v -w /hostlab/shared/.output/MU2_Gat
eway1_eth0.pcap > /dev/null 2>&1 &
[2] 1727
root@Gateway1:~# 
```

MU2_Gateway1_eth1.pcap

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

```
No.  Time      Source             Destination        Protocol Length Info
   1 0.000000  00:00:00_00:03:01  Broadcast          ARP        42 Who has 213.0.133.162? Tell 213.0.133.161
   2 0.000032  00:00:00_00:04:02  00:00:00_00:03:01  ARP        42 213.0.133.162 is at 00:00:00:00:04:02
   3 0.000309  22.39.222.2        213.0.133.162      WireGu…   190 Handshake Initiation, sender=0x09F99D30
   4 0.001287  213.0.133.162      22.39.222.2        WireGu…   134 Handshake Response, sender=0x68786961, receiver=0x09F99D30
   5 0.002079  22.39.222.2        213.0.133.162      WireGu…   170 Transport Data, receiver=0x68786961, counter=0, datalen=96
   6 0.002669  213.0.133.162      22.39.222.2        WireGu…   170 Transport Data, receiver=0x09F99D30, counter=0, datalen=96
   7 1.002059  22.39.222.2        213.0.133.162      WireGu…   170 Transport Data, receiver=0x68786961, counter=1, datalen=96
   8 1.002438  213.0.133.162      22.39.222.2        WireGu…   170 Transport Data, receiver=0x09F99D30, counter=1, datalen=96
   9 2.005463  22.39.222.2        213.0.133.162      WireGu…   170 Transport Data, receiver=0x68786961, counter=2, datalen=96
  10 2.005882  213.0.133.162      22.39.222.2        WireGu…   170 Transport Data, receiver=0x09F99D30, counter=2, datalen=96
  11 3.007194  22.39.222.2        213.0.133.162      WireGu…   170 Transport Data, receiver=0x68786961, counter=3, datalen=96
  12 3.007489  213.0.133.162      22.39.222.2        WireGu…   170 Transport Data, receiver=0x09F99D30, counter=3, datalen=96
  13 4.008727  22.39.222.2        213.0.133.162      WireGu…   170 Transport Data, receiver=0x68786961, counter=4, datalen=96
  14 4.009070  213.0.133.162      22.39.222.2        WireGu…   170 Transport Data, receiver=0x09F99D30, counter=4, datalen=96
  15 5.010618  22.39.222.2        213.0.133.162      WireGu…   170 Transport Data, receiver=0x68786961, counter=5, datalen=96
  16 5.010976  213.0.133.162      22.39.222.2        WireGu…   170 Transport Data, receiver=0x09F99D30, counter=5, datalen=96
  17 5.051494  00:00:00_00:04:02  00:00:00_00:03:01  ARP        42 Who has 213.0.133.161? Tell 213.0.133.162
  18 5.051759  00:00:00_00:03:01  00:00:00_00:04:02  ARP        42 213.0.133.161 is at 00:00:00:00:03:01
  19 6.012323  22.39.222.2        213.0.133.162      WireGu…   170 Transport Data, receiver=0x68786961, counter=6, datalen=96

› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
› Ethernet II, Src: 00:00:00_00:03:01 (00:00:00:00:03:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)
```

- MobileUser2-Wireguard-eth1 (/hostlab/shared/.output/MU2_Gateway1_eth1.pcap)



MobileUser2

```
root@MobileUser2:~# ping 192.168.80.4
PING 192.168.80.4 (192.168.80.4) 56(84) bytes of data.
64 bytes from 192.168.80.4: icmp_seq=1 ttl=63 time=1.26 ms
64 bytes from 192.168.80.4: icmp_seq=2 ttl=63 time=1.22 ms
64 bytes from 192.168.80.4: icmp_seq=3 ttl=63 time=1.12 ms
64 bytes from 192.168.80.4: icmp_seq=4 ttl=63 time=1.10 ms
64 bytes from 192.168.80.4: icmp_seq=5 ttl=63 time=1.28 ms
64 bytes from 192.168.80.4: icmp_seq=6 ttl=63 time=1.17 ms
```

Gateway1

```
root@Gateway1:~# nohup tcpdump -s0 -i eth1 -v -w /hostlab/shared/.output/MU2_Gat
eway1_eth1.pcap > /dev/null 2>&1 &
[1] 1726
root@Gateway1:~# nohup tcpdump -s0 -i eth0 -v -w /hostlab/shared/.output/MU2_Gat
eway1_eth0.pcap > /dev/null 2>&1 &
[2] 1727
root@Gateway1:~# 
```

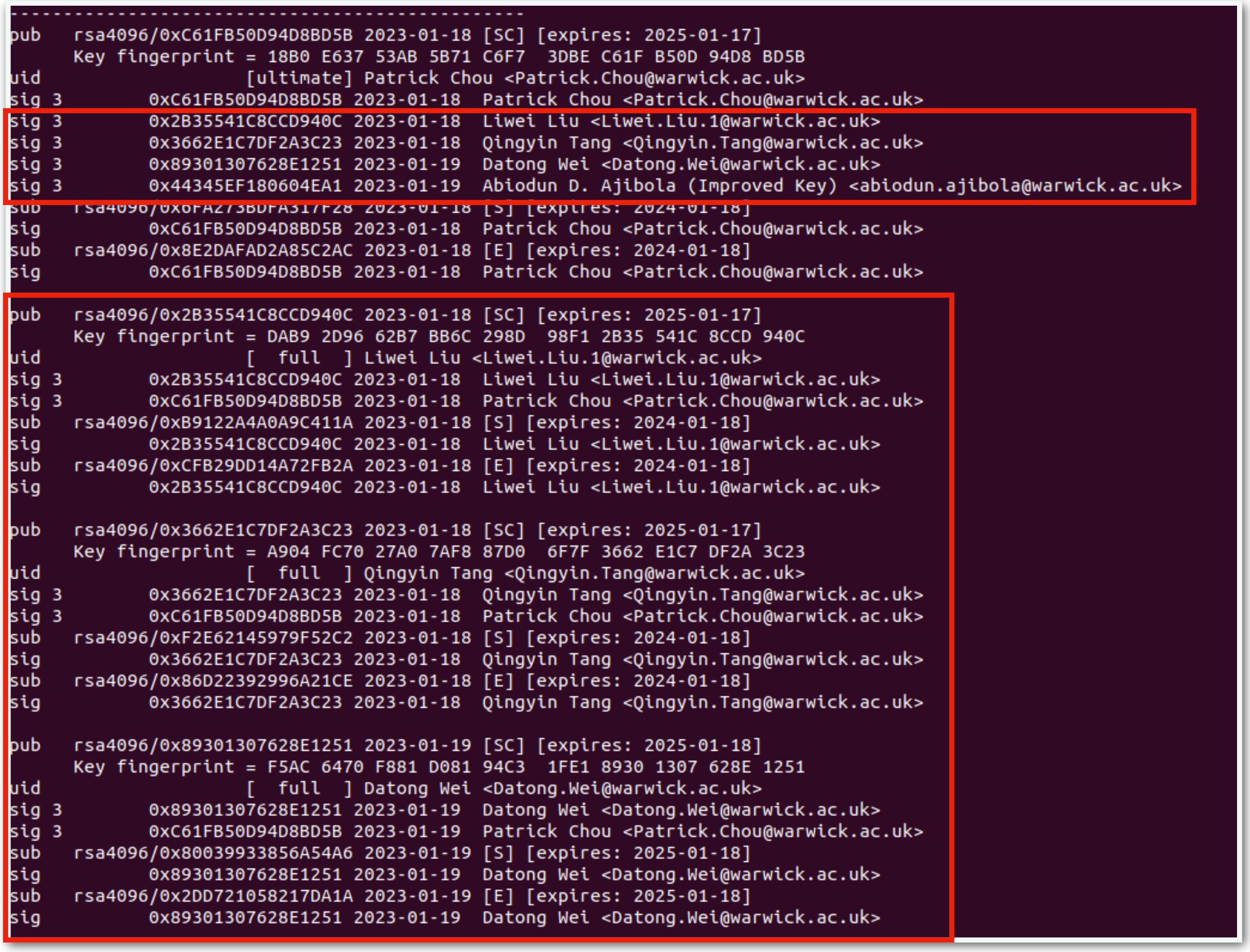
MU2_Gateway1_eth0.pcap

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

```
No.  Time      Source             Destination        Protocol Length Info
   1 0.000000  fe80::200:ff:fe00:4… ff02::2          ICMPv6     70 Router Solicitation from 00:00:00:00:04:01
   2 0.630558  00:00:00_00:04:01  Broadcast          ARP        42 Who has 192.168.80.4? Tell 192.168.80.1
   3 0.630811  00:00:00_00:07:01  00:00:00_00:04:01  ARP        42 192.168.80.4 is at 00:00:00:00:07:01
   4 0.630816  192.168.80.1       192.168.80.4       ICMP       98 Echo (ping) request  id=0x976a, seq=1/256, ttl=63 (reply in 5)
   5 0.631038  192.168.80.4       192.168.80.1       ICMP       98 Echo (ping) reply    id=0x976a, seq=1/256, ttl=64 (request in…
   6 1.630519  192.168.80.1       192.168.80.4       ICMP       98 Echo (ping) request  id=0x976a, seq=2/512, ttl=63 (reply in 7)
   7 1.630809  192.168.80.4       192.168.80.1       ICMP       98 Echo (ping) reply    id=0x976a, seq=2/512, ttl=64 (request in…
   8 2.633933  192.168.80.1       192.168.80.4       ICMP       98 Echo (ping) request  id=0x976a, seq=3/768, ttl=63 (reply in 9)
   9 2.634253  192.168.80.4       192.168.80.1       ICMP       98 Echo (ping) reply    id=0x976a, seq=3/768, ttl=64 (request in…
  10 3.635649  192.168.80.1       192.168.80.4       ICMP       98 Echo (ping) request  id=0x976a, seq=4/1024, ttl=63 (reply in …
  11 3.635865  192.168.80.4       192.168.80.1       ICMP       98 Echo (ping) reply    id=0x976a, seq=4/1024, ttl=64 (request i…
  12 4.637187  192.168.80.1       192.168.80.4       ICMP       98 Echo (ping) request  id=0x976a, seq=5/1280, ttl=63 (reply in …
  13 4.637450  192.168.80.4       192.168.80.1       ICMP       98 Echo (ping) reply    id=0x976a, seq=5/1280, ttl=64 (request i…
  14 5.639091  192.168.80.1       192.168.80.4       ICMP       98 Echo (ping) request  id=0x976a, seq=6/1536, ttl=63 (reply in …
  15 5.639346  192.168.80.4       192.168.80.1       ICMP       98 Echo (ping) reply    id=0x976a, seq=6/1536, ttl=64 (request i…
  16 5.656342  00:00:00_00:07:01  00:00:00_00:04:01  ARP        42 Who has 192.168.80.1? Tell 192.168.80.4
  17 5.656365  00:00:00_00:04:01  00:00:00_00:07:01  ARP        42 192.168.80.1 is at 00:00:00:00:04:01
  18 6.640782  192.168.80.1       192.168.80.4       ICMP       98 Echo (ping) request  id=0x976a, seq=7/1792, ttl=63 (reply in …
  19 6.640999  192.168.80.4       192.168.80.1       ICMP       98 Echo (ping) reply    id=0x976a, seq=7/1792, ttl=64 (request i…

› Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
› Ethernet II, Src: 00:00:00_00:04:01 (00:00:00:00:04:01), Dst: IPv6mcast_02 (33:33:00:00:00:02)
› Internet Protocol Version 6, Src: fe80::200:ff:fe00:401, Dst: ff02::2
› Internet Control Message Protocol v6
```

Phase2:

2.1 Have your submitted public key signed by at least three other students' submitted public keys, and have correctly used the private key associated with your submitted public key, to sign the submitted public keys of at least three other students in the class[1]



```
-------------------------------------------------
pub   rsa4096/0xC61FB50D94D8BD5B 2023-01-18 [SC] [expires: 2025-01-17]
      Key fingerprint = 18B0 E637 53AB 5B71 C6F7  3DBE C61F B50D 94D8 BD5B
uid                   [ultimate] Patrick Chou <Patrick.Chou@warwick.ac.uk>
sig 3        0xC61FB50D94D8BD5B 2023-01-18  Patrick Chou <Patrick.Chou@warwick.ac.uk>
sig 3        0x2B35541C8CCD940C 2023-01-18  Liwei Liu <Liwei.Liu.1@warwick.ac.uk>
sig 3        0x3662E1C7DF2A3C23 2023-01-18  Qingyin Tang <Qingyin.Tang@warwick.ac.uk>
sig 3        0x89301307628E1251 2023-01-19  Datong Wei <Datong.Wei@warwick.ac.uk>
sig 3        0x44345EF180604EA1 2023-01-19  Abiodun D. Ajibola (Improved Key) <abiodun.ajibola@warwick.ac.uk>
sub   rsa4096/0x6FA273BDFA317F28 2023-01-18 [S] [expires: 2024-01-18]
sig          0xC61FB50D94D8BD5B 2023-01-18  Patrick Chou <Patrick.Chou@warwick.ac.uk>
sub   rsa4096/0x8E2DAFAD2A85C2AC 2023-01-18 [E] [expires: 2024-01-18]
sig          0xC61FB50D94D8BD5B 2023-01-18  Patrick Chou <Patrick.Chou@warwick.ac.uk>

pub   rsa4096/0x2B35541C8CCD940C 2023-01-18 [SC] [expires: 2025-01-17]
      Key fingerprint = DAB9 2D96 62B7 BB6C 298D  98F1 2B35 541C 8CCD 940C
uid                   [  full  ] Liwei Liu <Liwei.Liu.1@warwick.ac.uk>
sig 3        0x2B35541C8CCD940C 2023-01-18  Liwei Liu <Liwei.Liu.1@warwick.ac.uk>
sig 3        0xC61FB50D94D8BD5B 2023-01-18  Patrick Chou <Patrick.Chou@warwick.ac.uk>
sub   rsa4096/0xB9122A4A0A9C411A 2023-01-18 [S] [expires: 2024-01-18]
sig          0x2B35541C8CCD940C 2023-01-18  Liwei Liu <Liwei.Liu.1@warwick.ac.uk>
sub   rsa4096/0xCFB29DD14A72FB2A 2023-01-18 [E] [expires: 2024-01-18]
sig          0x2B35541C8CCD940C 2023-01-18  Liwei Liu <Liwei.Liu.1@warwick.ac.uk>

pub   rsa4096/0x3662E1C7DF2A3C23 2023-01-18 [SC] [expires: 2025-01-17]
      Key fingerprint = A904 FC70 27A0 7AF8 87D0  6F7F 3662 E1C7 DF2A 3C23
uid                   [  full  ] Qingyin Tang <Qingyin.Tang@warwick.ac.uk>
sig 3        0x3662E1C7DF2A3C23 2023-01-18  Qingyin Tang <Qingyin.Tang@warwick.ac.uk>
sig 3        0xC61FB50D94D8BD5B 2023-01-18  Patrick Chou <Patrick.Chou@warwick.ac.uk>
sub   rsa4096/0xF2E62145979F52C2 2023-01-18 [S] [expires: 2024-01-18]
sig          0x3662E1C7DF2A3C23 2023-01-18  Qingyin Tang <Qingyin.Tang@warwick.ac.uk>
sub   rsa4096/0x86D22392996A21CE 2023-01-18 [E] [expires: 2024-01-18]
sig          0x3662E1C7DF2A3C23 2023-01-18  Qingyin Tang <Qingyin.Tang@warwick.ac.uk>

pub   rsa4096/0x89301307628E1251 2023-01-19 [SC] [expires: 2025-01-18]
      Key fingerprint = F5AC 6470 F881 D081 94C3  1FE1 8930 1307 628E 1251
uid                   [  full  ] Datong Wei <Datong.Wei@warwick.ac.uk>
sig 3        0x89301307628E1251 2023-01-19  Datong Wei <Datong.Wei@warwick.ac.uk>
sig 3        0xC61FB50D94D8BD5B 2023-01-19  Patrick Chou <Patrick.Chou@warwick.ac.uk>
sub   rsa4096/0x80039933856A54A6 2023-01-19 [S] [expires: 2025-01-18]
sig          0x89301307628E1251 2023-01-19  Datong Wei <Datong.Wei@warwick.ac.uk>
sub   rsa4096/0x2DD721058217DA1A 2023-01-19 [E] [expires: 2025-01-18]
sig          0x89301307628E1251 2023-01-19  Datong Wei <Datong.Wei@warwick.ac.uk>
```

3. Identifying the further work that is needed but that you were unable to realise

- Make a compelling case for your scalable design and implementation of the IPSec VPN using the x509 certificate authority hierarchy as appropriate, permitting multiple workers to achieve connectivity

4. Reference

[1] The Free Software Foundation. (1999) The GNU Privacy Handbook. Available from: https://www.gnupg.org/gph/en/manual.html

[2] Chandan Kumar. (2020) 21 OpenSSL Examples to Help You in Real-World. Available from: https://geekflare.com/openssl-commands-certificates/

[3] Greg Schafer. (2021) What They Don’t Tell You About Setting Up A WireGuard VPN. Available from: https://medium.com/tangram-visions/what-they-dont-tell-you-about-setting-up-a-wireguard-vpn-46f7bd168478