

CDP PMA

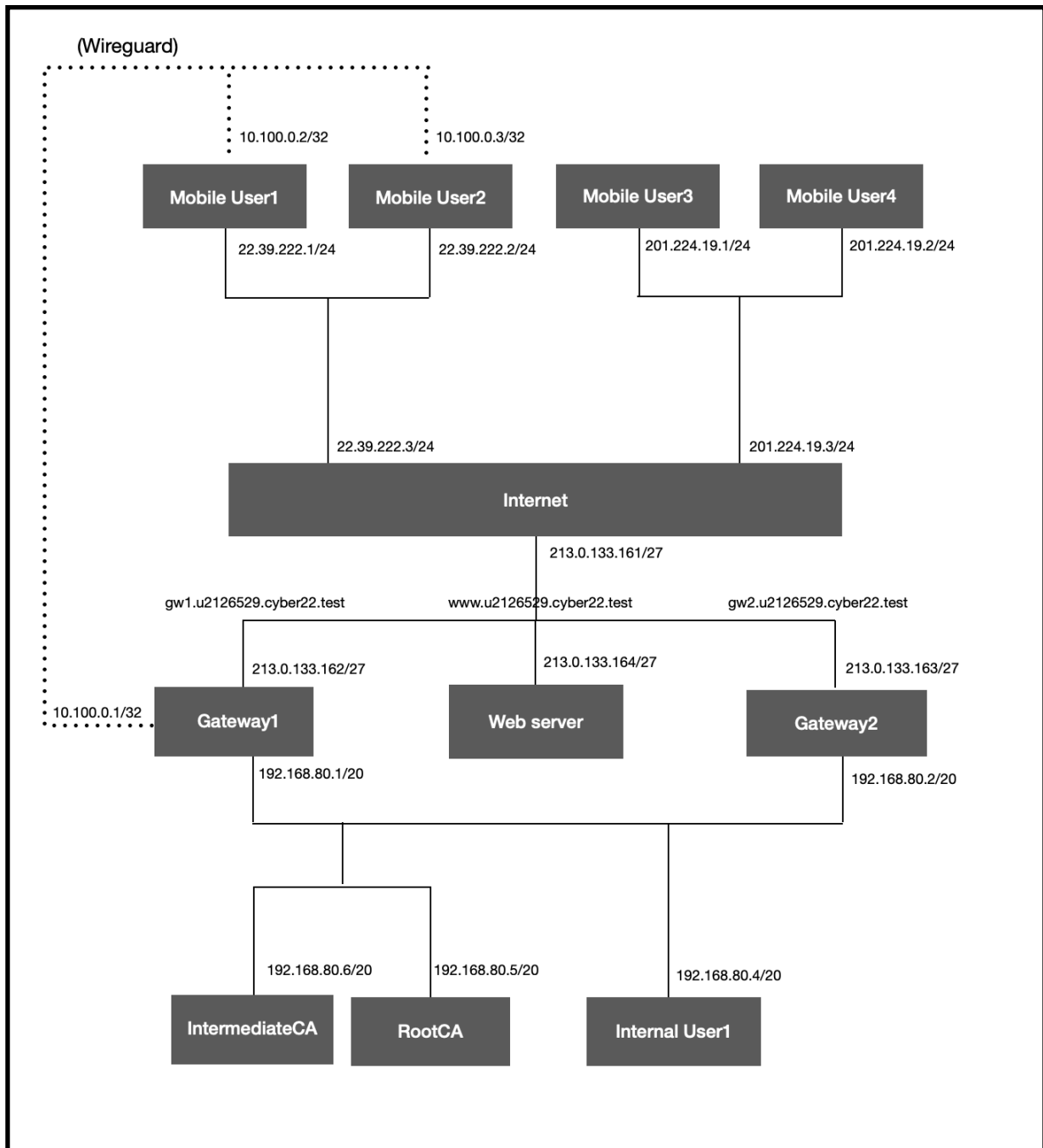
Student ID or IDs for group work	2126529
Module Date	12th - 16th December 2022
GPG Fingerprint	18B0 E637 53AB 5B71 C6F7 3DBE C61F B50D 94D8 BD5B

Date set	16 th Dec 2022
Submission date (excluding extensions)	23 rd 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

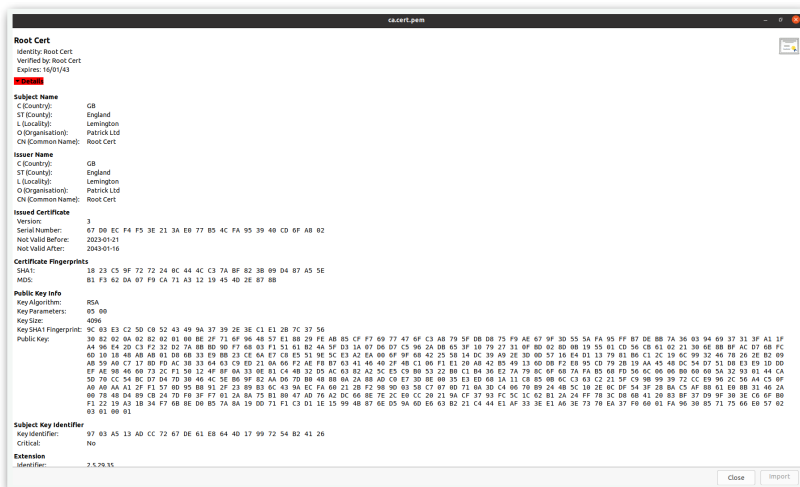
1.3 Define and implement a credible x509 certificate hierarchy for the organisation, consistent with the script of instructions used to achieve this[2]

1.3.1 Certificate hierarchy: Root - Intermediate - Server

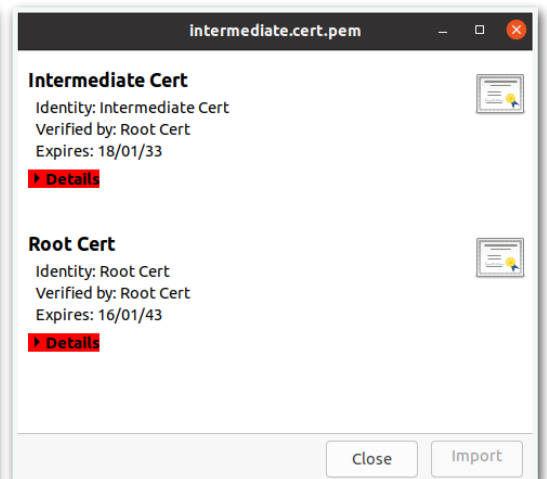
```
cdp22
|
|--create-x509.sh (this script)
|
|--RootCA
|   |
|   |--ca
|   |   |
|   |   |--root
|   |   |   |
|   |   |   |--openssl.cnf (config for a root ca)
|   |   |   |
|   |   |   |--(various dirs, certs and keys)
|   |
|--intermediateCA
|   |
|   |--ca
|   |   |
|   |   |--intermediate
|   |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

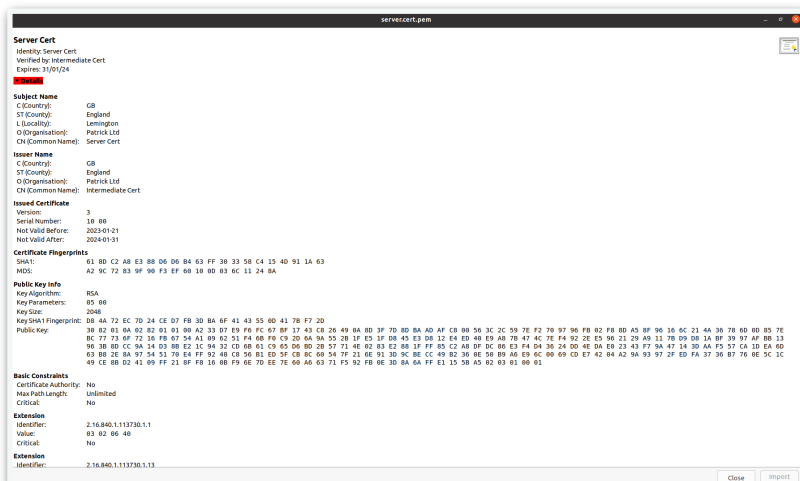
- Root cert (RootCA/ca/root/certs/ca.cert.pem):



- Intermediate cert and CA Chain (IntermediateCA/ca/root/certs/Intermediate.cert.pem):
- We use CA chain to verify server cert by intermediate cert



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



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 rsa4096/0x6FA273BDF4317F28 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)

The screenshot shows two terminal windows and a Wireshark capture. The MobileUser1 terminal shows a successful ping to 192.168.80.4. The Gateway1 terminal shows the execution of tcpdump on eth1. The Wireshark capture, titled 'MU1_Gateway1_eth1.pcap', shows a WireGuard handshake between 22.39.222.1 and 213.0.133.162, followed by several transport data packets. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	22.39.222.1	213.0.133.162	WireGu.	130	Handshake Initiation, sender=9x98370D30
2	0.000593	213.0.133.162	22.39.222.1	WireGu.	134	Handshake Response, sender=0x7EA386F6, receiver=0x98370D30
3	0.001204	22.39.222.1	213.0.133.162	WireGu.	170	Transport Data, receiver=0x7EA386F6, counter=0, datalen=96
4	0.001485	213.0.133.162	22.39.222.1	WireGu.	170	Transport Data, receiver=0x98370D30, counter=0, datalen=96
5	0.001302	22.39.222.1	213.0.133.162	WireGu.	170	Transport Data, receiver=0x7EA386F6, counter=1, datalen=96
6	0.001713	213.0.133.162	22.39.222.1	WireGu.	170	Transport Data, receiver=0x98370D30, counter=1, datalen=96
7	0.005600	22.39.222.1	213.0.133.162	WireGu.	170	Transport Data, receiver=0x7EA386F6, counter=2, datalen=96
8	0.005904	213.0.133.162	22.39.222.1	WireGu.	170	Transport Data, receiver=0x98370D30, counter=2, datalen=96
9	0.007457	22.39.222.1	213.0.133.162	WireGu.	170	Transport Data, receiver=0x7EA386F6, counter=3, datalen=96
10	0.007896	213.0.133.162	22.39.222.1	WireGu.	170	Transport Data, receiver=0x98370D30, counter=3, datalen=96
11	0.011561	22.39.222.1	213.0.133.162	WireGu.	170	Transport Data, receiver=0x7EA386F6, counter=4, datalen=96
12	0.011929	213.0.133.162	22.39.222.1	WireGu.	170	Transport Data, receiver=0x98370D30, counter=4, datalen=96
13	0.011377	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	0.011388	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	0.014534	22.39.222.1	213.0.133.162	WireGu.	170	Transport Data, receiver=0x7EA386F6, counter=5, datalen=96
16	0.014898	213.0.133.162	22.39.222.1	WireGu.	170	Transport Data, receiver=0x98370D30, counter=5, datalen=96
17	0.078685	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	0.079016	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	0.018603	22.39.222.1	213.0.133.162	WireGu.	170	Transport Data, receiver=0x7EA386F6, counter=6, datalen=96

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

The screenshot shows two terminal windows and a Wireshark capture. The MobileUser1 terminal shows a successful ping to 192.168.80.4. The Gateway1 terminal shows the execution of tcpdump on eth0. The Wireshark capture, titled 'MU1_Gateway1_eth0.pcap', shows a series of ICMP echo requests and replies between 192.168.80.1 and 192.168.80.4. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.80.1	192.168.80.4	ICMP	60	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	0.000154	192.168.80.1	192.168.80.4	ICMP	98	Echo (ping) request id=0x3338, seq=2/512, ttl=63 (reply in 4)
4	0.000420	192.168.80.4	192.168.80.1	ICMP	98	Echo (ping) reply id=0x3338, seq=2/512, ttl=64 (request in ...)
5	0.004488	192.168.80.1	192.168.80.4	ICMP	98	Echo (ping) request id=0x3338, seq=3/768, ttl=63 (reply in 6)
6	0.004634	192.168.80.4	192.168.80.1	ICMP	98	Echo (ping) reply id=0x3338, seq=3/768, ttl=64 (request in ...)
7	0.006271	192.168.80.1	192.168.80.4	ICMP	98	Echo (ping) request id=0x3338, seq=4/1024, ttl=63 (reply in ...)
8	0.006618	192.168.80.4	192.168.80.1	ICMP	98	Echo (ping) reply id=0x3338, seq=4/1024, ttl=64 (request in ...)
9	0.010376	192.168.80.1	192.168.80.4	ICMP	98	Echo (ping) request id=0x3338, seq=5/1280, ttl=63 (reply in ...)
10	0.010654	192.168.80.4	192.168.80.1	ICMP	98	Echo (ping) reply id=0x3338, seq=5/1280, ttl=64 (request in ...)
11	0.013355	192.168.80.1	192.168.80.4	ICMP	98	Echo (ping) request id=0x3338, seq=6/1536, ttl=63 (reply in ...)
12	0.013626	192.168.80.4	192.168.80.1	ICMP	98	Echo (ping) reply id=0x3338, seq=6/1536, ttl=64 (request in ...)
13	0.054255	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	0.054268	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	0.077417	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	0.077720	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	0.017414	192.168.80.1	192.168.80.4	ICMP	98	Echo (ping) request id=0x3338, seq=7/1792, ttl=63 (reply in ...)
18	0.017733	192.168.80.4	192.168.80.1	ICMP	98	Echo (ping) reply id=0x3338, seq=7/1792, ttl=64 (request in ...)
19	0.022509	192.168.80.1	192.168.80.4	ICMP	98	Echo (ping) request id=0x3338, seq=8/2048, ttl=63 (reply in ...)

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)

The screenshot shows a terminal window with two sessions: MobileUser2 and Gateway1. MobileUser2 is running a ping command to 192.168.80.4. Gateway1 is running tcpdump on eth1 to capture traffic. Below the terminal is a Wireshark capture of MU2_Gateway1_eth1.pcap. The capture shows a series of ICMP Echo (ping) requests and responses between 22.39.222.2 and 213.0.133.162. The first frame is highlighted, showing the ICMP Echo request from 22.39.222.2 to 213.0.133.162.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	22.39.222.2	213.0.133.162	WireGuard	42	Who has 213.0.133.162? Tell 213.0.133.162
2	0.000000	213.0.133.162	22.39.222.2	WireGuard	190	Handshake Initiation, sender=0x09f99030
3	0.000000	213.0.133.162	22.39.222.2	WireGuard	134	Handshake Response, sender=0x68786961, receiver=0x09f99030
4	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=0, datalen=96
5	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=1, datalen=96
6	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=2, datalen=96
7	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=3, datalen=96
8	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=4, datalen=96
9	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=5, datalen=96
10	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=6, datalen=96
11	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=7, datalen=96
12	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=8, datalen=96
13	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=9, datalen=96
14	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=10, datalen=96
15	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=11, datalen=96
16	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=12, datalen=96
17	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=13, datalen=96
18	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=14, datalen=96
19	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=15, datalen=96
20	0.000000	213.0.133.162	22.39.222.2	WireGuard	170	Transport Data, receiver=0x09f99030, counter=16, datalen=96

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

The screenshot shows a terminal window with two sessions: MobileUser2 and Gateway1. MobileUser2 is running a ping command to 192.168.80.4. Gateway1 is running tcpdump on eth0 to capture traffic. Below the terminal is a Wireshark capture of MU2_Gateway1_eth0.pcap. The capture shows a series of ICMP Echo (ping) requests and responses between 192.168.80.1 and 192.168.80.4. The first frame is highlighted, showing the ICMP Echo request from 192.168.80.1 to 192.168.80.4.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.80.1	192.168.80.4	ICMPv6	78	Router Solicitation from 00:00:00:00:00:00
2	0.000000	192.168.80.4	192.168.80.1	ICMPv6	42	Who has 192.168.80.4? Tell 192.168.80.1
3	0.000000	192.168.80.1	192.168.80.4	ICMPv6	42	192.168.80.4 is at 00:00:00:00:00:00
4	0.000000	192.168.80.1	192.168.80.4	ICMPv6	98	Echo (ping) request id=0x976a, seq=1/256, ttl=63 (reply in 5)
5	0.000000	192.168.80.4	192.168.80.1	ICMPv6	98	Echo (ping) reply id=0x976a, seq=1/256, ttl=63 (request in 5)
6	0.000000	192.168.80.1	192.168.80.4	ICMPv6	98	Echo (ping) request id=0x976a, seq=2/512, ttl=63 (reply in 7)
7	0.000000	192.168.80.4	192.168.80.1	ICMPv6	98	Echo (ping) reply id=0x976a, seq=2/512, ttl=63 (request in 7)
8	0.000000	192.168.80.1	192.168.80.4	ICMPv6	98	Echo (ping) request id=0x976a, seq=3/768, ttl=63 (reply in 9)
9	0.000000	192.168.80.4	192.168.80.1	ICMPv6	98	Echo (ping) reply id=0x976a, seq=3/768, ttl=63 (request in 9)
10	0.000000	192.168.80.1	192.168.80.4	ICMPv6	98	Echo (ping) request id=0x976a, seq=4/1024, ttl=63 (reply in 11)
11	0.000000	192.168.80.4	192.168.80.1	ICMPv6	98	Echo (ping) reply id=0x976a, seq=4/1024, ttl=63 (request in 11)
12	0.000000	192.168.80.1	192.168.80.4	ICMPv6	98	Echo (ping) request id=0x976a, seq=5/1280, ttl=63 (reply in 13)
13	0.000000	192.168.80.4	192.168.80.1	ICMPv6	98	Echo (ping) reply id=0x976a, seq=5/1280, ttl=63 (request in 13)
14	0.000000	192.168.80.1	192.168.80.4	ICMPv6	98	Echo (ping) request id=0x976a, seq=6/1536, ttl=63 (reply in 15)
15	0.000000	192.168.80.4	192.168.80.1	ICMPv6	98	Echo (ping) reply id=0x976a, seq=6/1536, ttl=63 (request in 15)
16	0.000000	192.168.80.1	192.168.80.4	ICMPv6	98	Echo (ping) request id=0x976a, seq=7/1792, ttl=63 (reply in 17)
17	0.000000	192.168.80.4	192.168.80.1	ICMPv6	98	Echo (ping) reply id=0x976a, seq=7/1792, ttl=63 (request in 17)
18	0.000000	192.168.80.1	192.168.80.4	ICMPv6	98	Echo (ping) request id=0x976a, seq=8/2048, ttl=63 (reply in 19)
19	0.000000	192.168.80.4	192.168.80.1	ICMPv6	98	Echo (ping) reply id=0x976a, seq=8/2048, ttl=63 (request in 19)
20	0.000000	192.168.80.1	192.168.80.4	ICMPv6	98	Echo (ping) request id=0x976a, seq=9/2304, ttl=63 (reply in 21)
21	0.000000	192.168.80.4	192.168.80.1	ICMPv6	98	Echo (ping) reply id=0x976a, seq=9/2304, ttl=63 (request in 21)

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  rsa4096/0xC61FB50D94D8BD5B 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>