Most used commands

curl:

curl --cacert "d:\ws meetup\cert\root-ca.crt" --ssl-no-revoke https://bad.koene.tld
curl --cacert "d:\ws meetup\cert\root-ca.crt" --ssl-no-revoke https://good.koene.tld

curl -kivL --resolve bad.koene.tld:443:192.168.0.124 --cacert "d:\ws meetup\cert\root-ca.crt" --ssl-no-revoke https://bad.koene.tld

-k = no certificate check
-I = only http headers
-v = verbose
-L = follow redirects
--resolve = fill DNS cache

curl --help all

openssl:

openssl s_client -servername good.koene.tld -connect 192.168.0.42:443

F5 session key tcpdump command (K31793632):

First enable SSL option:
tmsh modify sys db tcpdump.sslprovider value enable

Then tcpdump
tcpdump --f5 ssl -nni 0.0:nnnp -vvvt -s 0 -w /var/tmp/bad.pcap host 192.168.0.24
tcpdump --f5 ssl -nni 0.0:nnnp -vvvt -s 0 -w /var/tmp/good.pcap host 192.168.0.42

Finally disable SSL option:
tmsh modify sys db tcpdump.sslprovider value disable

F5 session key irule (K12783074):

https://my.f5.com/manage/s/article/K12783074

tshark session key extraction command:

```
tshark -r decrypt.pcap -Y f5ethtrailer.tls.keylog -Tfields -e f5ethtrailer.tls.keylog | sed 's/,/\n/g' > ./pre_master_log.pms
```

Wireshark display filters:

TLS handshake packets:

```
tls.handshake
```

Check if the pcap contains the session keys:

```
tls && frame matches "\xf5\xde\xb0\xf5....\x00\x04\x00\x00"
```

Select the packet(s) containing the session keys:

```
f5ethtrailer.tls.keylog
```

Manual extraction of session keys from pcap file:

Set display filter:

```
f5ethtrailer.tls.keylog
```

Go to:

```
>F5 Ethernet Trailer Protocol
        > F5 TLS
```

Copy all 4 keylog entries to pms file.

Environment vars Win11:

rundll32.exe sysdm.cpl,EditEnvironmentVariables

Recources

RFC's:

- RSA : RFC 8017
- DH : RFC 2631
- ECDH : RFC 8422 (TLS 1.2)
- ECDHE : RFC 8422 (TLS 1.2) & RFC 8446 (TLS1.3)

Youtube:

Elliptic Curve : F5 lightboard lesson by John Wagnon on YT

F5 KB's:

TLS decryption irule: K12783074

K411: Overview of packet tracing with the tcpdump utility

K13637: Capturing internal TMM information with tcpdump

NCSC

ICT-beveiligingsrichtlijnen voor TLS v2.1, bijlage A