Activity 1

Network traffic analysis

The goal of this activity is to analyze the traffic generated by a smartphone app.
In order to do this, the traffic generated by the application *MyUnits* has been analyzed.

Setup

- *Windows* 10 laptop
- A*ndroid* 10 smartphone
- Home wifi
- *Wireshark* version 3.6.3
- *mitmproxy* version 8.0.0

Description

A PC was connected to home wifi and was configured to operate as a hotspot.
A smartphone was connected to the hotspot network and the *Wireshark* application was started on the PC to record the traffic. The *MyUnits* application was started on the smartphone, in order to generate traffic that can be analyzed.

By inspecting the traffic, it is possible to derive the following:

DNS
Two DNS requests were sent by the smartphone to the DNS server in order to retrieve the IP addresses that are associated with the domains “apilocator.appstudenti.cineca.it” and “units-prod.appstudenti.units.it”.
Both the responses provide a CNAME type RR and an additional A type record (figure 1,2).
In both cases, the CNAME type RR points to "osroute-prod-1.cineca.it" and the A type RR provides the IP address "130.186.6.97".

TCP
After each DNS request, the TCP three-way-handshake is recorded (figure 3) and the smartphone establishes a TCP connection with the server at the address 130.186.6.97, on port 443, which means that the HTTPS protocol is adopted.

TLS
Thereafter, the TLS Handshake is recorded. In both cases, the server sends a certificate chain which is composed of three certificates (figure 4), as illustrated in the following table.

Subject	**Issuer**
USERTrust RSA Certification Authority	AAA Certificate Services
Sectigo RSA Organization Validation Secure Ser	USERTrust RSA Certification Authority
* .appstudenti.cineca.it	Sectigo RSA Organization Validation Secure Ser

"AAA Certificate Services" is the trust anchor of the certificate chain and it is possible to verify that the certificate is present in the TrustSet of the smartphone (figure 5).

Following the above analysis, an analysis of the HTTP requests was conducted.
The *mitmproxy* application was started on the PC and the smartphone was connected to the home wifi through a proxy.
The smartphone proxy settings were configured by providing the IP address of the PC and the port on which *mitmproxy* was running (figure 6,7,8). The *mitmproxy CA* certificate was installed on the smartphone.

By this analysis, it is possible to derive the following:

API & Authentication
The application receives data from the API with the base url "units-prod.appstudenti.cineca.it" and the authentication protocol is Basic Authentication over HTTPS (figure 9).

Certificate Pinning
Some applications employ Certificate Pinning to prevent man-in-the-middle attacks.
This means that *mitmproxy's* certificate will not be accepted by these applications.
In the current study, the application was working properly and therefore it follows that Certificate Pinning is not adopted.

Other considerations:

MFA
The application does not support MFA.

Activity 2

MITM demo

The goal of this activity is to demonstrate a form of Man-In-The-Middle attack against a smartphone browser.

Setup

- *Windows* 10 laptop
- *Android* 10 smartphone
- Home wifi
- *Wireshark* version 3.6.3
- *Technitium* DNS Server version 8.1
- *Abyss* Web Server X1 version 2.16.1.9
- *Firefox* browser version 100.1.1

Description

- A PC is connected to the home wifi and acts as a hotspot
- A Web Server and a DNS Server are installed on the PC
- A smartphone is connected to the hotspot network
- The smartphone browser sends an HTTP or an HTTPS request to the website "www.unive.it"
- The DNS Server installed on the PC intercepts the request and redirects the browser to the Web Server installed on the PC
- A simple HTML template that differs from the original site is displayed on the browser
- *Wireshark* is used to analyze traffic

PC Configuration

- I installed *Technitium* Dns Server on the PC
- I installed *Abyss* Web Server on the PC
- I modified Network Connection settings so that the DNS server is not detected automatically but is inserted statically. Then, I inserted the IP address of the computer in the hotspot network, i.e. 192.168.137.1 (figure 10)

Web Server Configuration

- I put the HTML file of the web page, named index.html, in the appropriate directory, i.e. *htdocs*
- I generated a private key and a self-signed certificate through the *Abyss* console (figure 11)

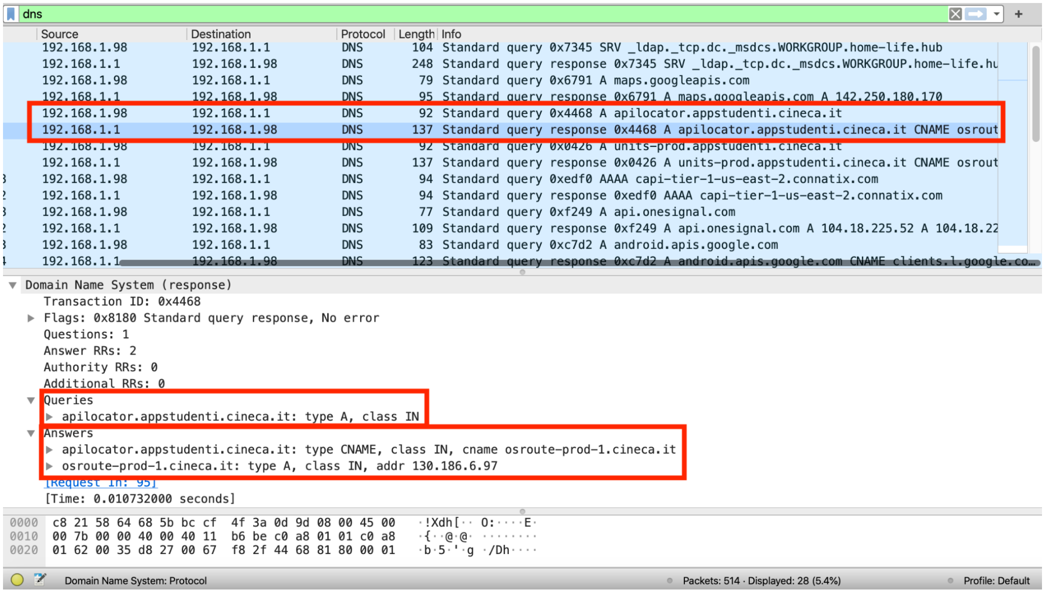
- I configured the host to be accessible with HTTP and HTTPS (figure 12)
- I configured the host name as "www.unive.it" in the Web Server General settings (figure 12)
- I configured the server to run TLS v1.2 in order to be sure to observe the certificate while inspecting the network traffic

DNS Server Configuration

- I created a new zone called "unive.it" (figure 13)
- I inserted a new record: www A 192.168.137.1 (figure 14)

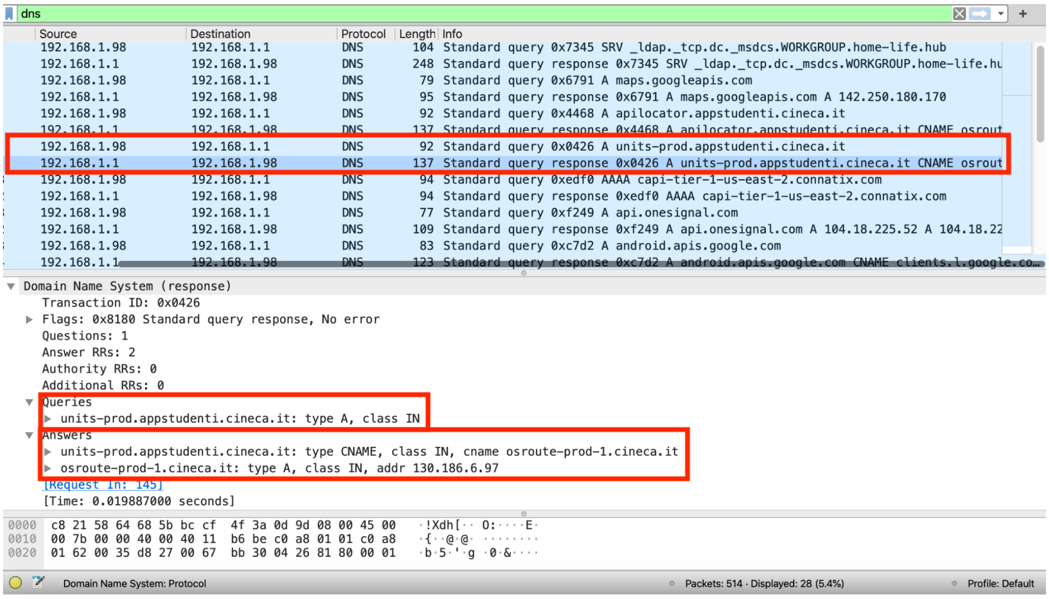
Appendix

Figures



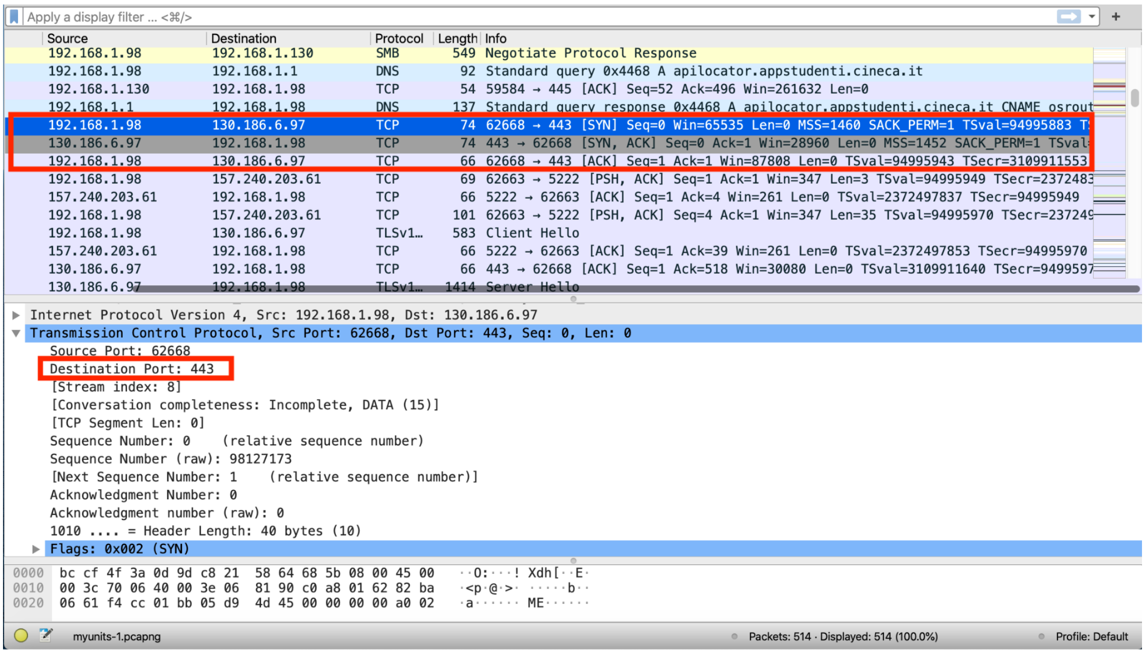
```
dns
Source          Destination     Protocol Length Info
192.168.1.98    192.168.1.1     DNS      104 Standard query 0x7345 SRV _ldap._tcp.dc._msdcs.WORKGROUP.home-life.hub
192.168.1.1     192.168.1.98    DNS      248 Standard query response 0x7345 SRV _ldap._tcp.dc._msdcs.WORKGROUP.home-life.hu
192.168.1.98    192.168.1.1     DNS       79 Standard query 0x6791 A maps.googleapis.com
192.168.1.1     192.168.1.98    DNS       95 Standard query response 0x6791 A maps.googleapis.com A 142.250.180.170
192.168.1.98    192.168.1.1     DNS       92 Standard query 0x4468 A apilocator.appstudenti.cineca.it
192.168.1.1     192.168.1.98    DNS      137 Standard query response 0x4468 A apilocator.appstudenti.cineca.it CNAME osrout
192.168.1.98    192.168.1.1     DNS       92 Standard query 0x0426 A units-prod.appstudenti.cineca.it
192.168.1.1     192.168.1.98    DNS      137 Standard query response 0x0426 A units-prod.appstudenti.cineca.it CNAME osrout
192.168.1.98    192.168.1.1     DNS       94 Standard query 0xedf0 AAAA capi-tier-1-us-east-2.connatix.com
192.168.1.1     192.168.1.98    DNS       94 Standard query response 0xedf0 AAAA capi-tier-1-us-east-2.connatix.com
192.168.1.98    192.168.1.1     DNS       77 Standard query 0xf249 A api.onesignal.com
192.168.1.1     192.168.1.98    DNS      109 Standard query response 0xf249 A api.onesignal.com A 104.18.225.52 A 104.18.22
192.168.1.98    192.168.1.1     DNS       83 Standard query 0xc7d2 A android.apis.google.com
192.168.1.1     192.168.1.98    DNS      123 Standard query response 0xc7d2 A android.apis.google.com CNAME clients.l.google.co…

▼ Domain Name System (response)
    Transaction ID: 0x4468
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ apilocator.appstudenti.cineca.it: type A, class IN
  ▼ Answers
    ▶ apilocator.appstudenti.cineca.it: type CNAME, class IN, cname osroute-prod-1.cineca.it
    ▶ osroute-prod-1.cineca.it: type A, class IN, addr 130.186.6.97
    [Request In: 95]
    [Time: 0.010732000 seconds]

0000  c8 21 58 64 68 5b bc cf  4f 3a 0d 9d 08 00 45 00   ·!Xdh[·· O:····E·
0010  00 7b 00 00 40 00 40 11  b6 be c0 a8 01 01 c0 a8   ·{··@·@· ········
0020  01 62 00 35 d8 27 00 67  f8 2f 44 68 81 80 00 01   ·b·5·'·g ·/Dh····

Domain Name System: Protocol          Packets: 514 · Displayed: 28 (5.4%)          Profile: Default
```

Figure 1: first DNS request



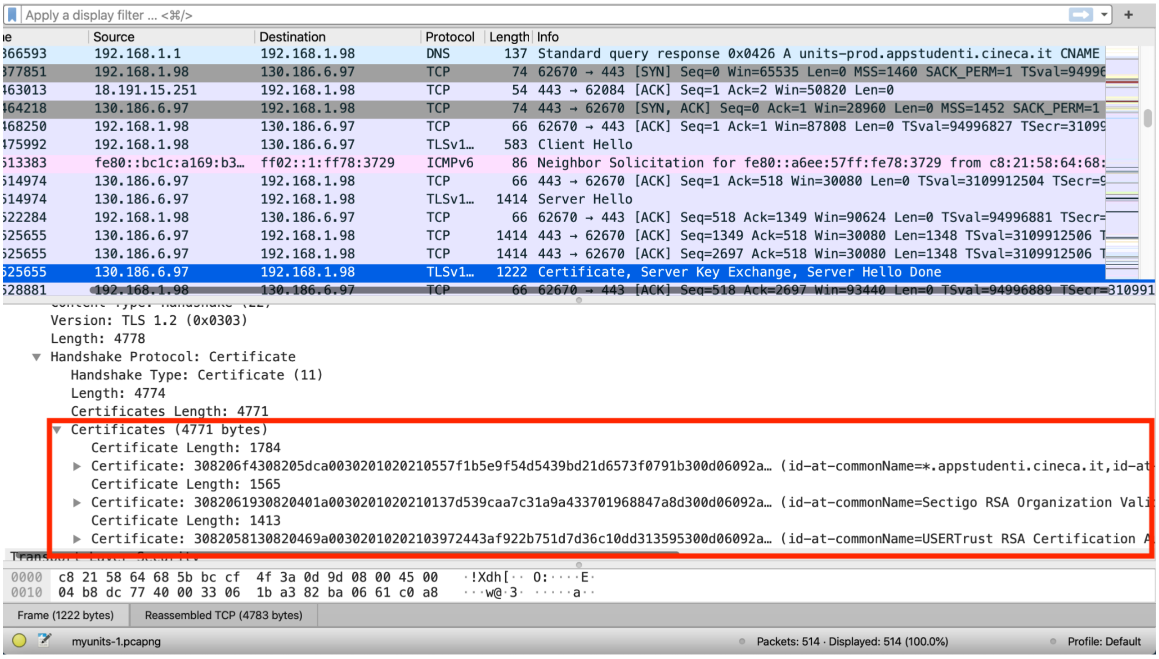
```
dns
Source          Destination     Protocol Length Info
192.168.1.98    192.168.1.1     DNS      104 Standard query 0x7345 SRV _ldap._tcp.dc._msdcs.WORKGROUP.home-life.hub
192.168.1.1     192.168.1.98    DNS      248 Standard query response 0x7345 SRV _ldap._tcp.dc._msdcs.WORKGROUP.home-life.hu
192.168.1.98    192.168.1.1     DNS       79 Standard query 0x6791 A maps.googleapis.com
192.168.1.1     192.168.1.98    DNS       95 Standard query response 0x6791 A maps.googleapis.com A 142.250.180.170
192.168.1.98    192.168.1.1     DNS       92 Standard query 0x4468 A apilocator.appstudenti.cineca.it
192.168.1.1     192.168.1.98    DNS      137 Standard query response 0x4468 A apilocator.appstudenti.cineca.it CNAME osrout
192.168.1.98    192.168.1.1     DNS       92 Standard query 0x0426 A units-prod.appstudenti.cineca.it
192.168.1.1     192.168.1.98    DNS      137 Standard query response 0x0426 A units-prod.appstudenti.cineca.it CNAME osrout
192.168.1.98    192.168.1.1     DNS       94 Standard query 0xedf0 AAAA capi-tier-1-us-east-2.connatix.com
192.168.1.1     192.168.1.98    DNS       94 Standard query response 0xedf0 AAAA capi-tier-1-us-east-2.connatix.com
192.168.1.98    192.168.1.1     DNS       77 Standard query 0xf249 A api.onesignal.com
192.168.1.1     192.168.1.98    DNS      109 Standard query response 0xf249 A api.onesignal.com A 104.18.225.52 A 104.18.22
192.168.1.98    192.168.1.1     DNS       83 Standard query 0xc7d2 A android.apis.google.com
192.168.1.1     192.168.1.98    DNS      123 Standard query response 0xc7d2 A android.apis.google.com CNAME clients.l.google.co…

▼ Domain Name System (response)
    Transaction ID: 0x0426
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ units-prod.appstudenti.cineca.it: type A, class IN
  ▼ Answers
    ▶ units-prod.appstudenti.cineca.it: type CNAME, class IN, cname osroute-prod-1.cineca.it
    ▶ osroute-prod-1.cineca.it: type A, class IN, addr 130.186.6.97
    [Request In: 145]
    [Time: 0.019887000 seconds]

0000  c8 21 58 64 68 5b bc cf  4f 3a 0d 9d 08 00 45 00   ·!Xdh[·· O:····E·
0010  00 7b 00 00 40 00 40 11  b6 be c0 a8 01 01 c0 a8   ·{··@·@· ········
0020  01 62 00 35 d8 27 00 67  bb 30 04 26 81 80 00 01   ·b·5·'·g ·0·&····

Domain Name System: Protocol          Packets: 514 · Displayed: 28 (5.4%)          Profile: Default
```

Figure 2: second DNS request



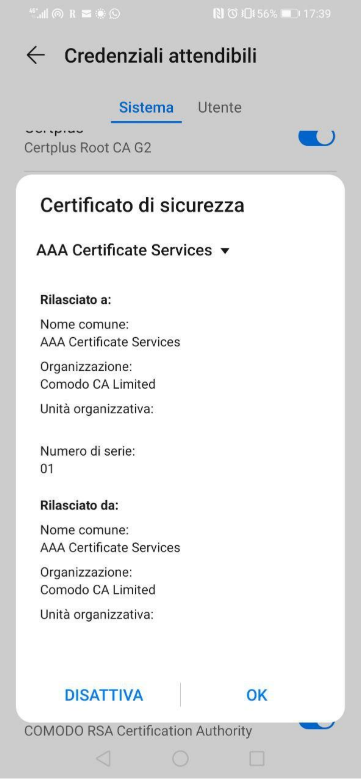
```
Apply a display filter ... <⌘/>

Source          Destination     Protocol Length Info
192.168.1.98    192.168.1.130   SMB        549 Negotiate Protocol Response
192.168.1.98    192.168.1.1     DNS         92 Standard query 0x4468 A apilocator.appstudenti.cineca.it
192.168.1.130   192.168.1.98    TCP         54 59584 → 445 [ACK] Seq=52 Ack=496 Win=261632 Len=0
192.168.1.1     192.168.1.98    DNS        137 Standard query response 0x4468 A apilocator.appstudenti.cineca.it CNAME osrout
192.168.1.98    130.186.6.97    TCP         74 62668 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=94995883 T
130.186.6.97    192.168.1.98    TCP         74 443 → 62668 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval
192.168.1.98    130.186.6.97    TCP         66 62668 → 443 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSval=94995943 TSecr=3109911553
192.168.1.98    157.240.203.61  TCP         69 62663 → 5222 [PSH, ACK] Seq=1 Ack=1 Win=347 Len=3 TSval=94995949 TSecr=2372483
157.240.203.61  192.168.1.98    TCP         66 5222 → 62663 [ACK] Seq=1 Ack=4 Win=261 Len=0 TSval=2372497837 TSecr=94995949
192.168.1.98    157.240.203.61  TCP        101 62663 → 5222 [PSH, ACK] Seq=4 Ack=1 Win=347 Len=35 TSval=94995970 TSecr=237249
192.168.1.98    130.186.6.97    TLSv1…     583 Client Hello
157.240.203.61  192.168.1.98    TCP         66 5222 → 62663 [ACK] Seq=1 Ack=39 Win=261 Len=0 TSval=2372497853 TSecr=94995970
130.186.6.97    192.168.1.98    TCP         66 443 → 62668 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=3109911640 TSecr=9499597
130.186.6.97    192.168.1.98    TLSv1…    1414 Server Hello

▶ Internet Protocol Version 4, Src: 192.168.1.98, Dst: 130.186.6.97
▼ Transmission Control Protocol, Src Port: 62668, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 62668
    Destination Port: 443
    [Stream index: 8]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 98127173
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  ▶ Flags: 0x002 (SYN)

0000  bc cf 4f 3a 0d 9d c8 21  58 64 68 5b 08 00 45 00   ··O:···! Xdh[··E·
0010  00 3c 70 06 40 00 3e 06  81 90 c0 a8 01 62 82 ba   ·<p·@·>· ·····b··
0020  06 61 f4 cc 01 bb 05 d9  4d 45 00 00 00 00 a0 02   ·a······ ME······

myunits-1.pcapng        Packets: 514 · Displayed: 514 (100.0%)        Profile: Default
```

Figure 3: TCP Handshake



```
Apply a display filter ... <⌘/>

ie      Source              Destination        Protocol Length Info
366593  192.168.1.1         192.168.1.98       DNS        137 Standard query response 0x0426 A units-prod.appstudenti.cineca.it CNAME
377851  192.168.1.98        130.186.6.97       TCP         74 62670 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=94996
463013  18.191.15.251       192.168.1.98       TCP         54 443 → 62084 [ACK] Seq=1 Ack=2 Win=50820 Len=0
464218  130.186.6.97        192.168.1.98       TCP         74 443 → 62670 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1
468250  192.168.1.98        130.186.6.97       TCP         66 62670 → 443 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSval=94996827 TSecr=31099
475992  192.168.1.98        130.186.6.97       TLSv1…     583 Client Hello
513383  fe80::bc1c:a169:b3… ff02::1:ff78:3729  ICMPv6      86 Neighbor Solicitation for fe80::a6ee:57ff:fe78:3729 from c8:21:58:64:68:
514974  130.186.6.97        192.168.1.98       TCP         66 443 → 62670 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=3109912504 TSecr=9
514974  130.186.6.97        192.168.1.98       TLSv1…    1414 Server Hello
522284  192.168.1.98        130.186.6.97       TCP         66 62670 → 443 [ACK] Seq=518 Ack=1349 Win=90624 Len=0 TSval=94996881 TSecr=
525655  130.186.6.97        192.168.1.98       TCP       1414 443 → 62670 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=3109912506 T
525655  130.186.6.97        192.168.1.98       TCP       1414 443 → 62670 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=3109912506 T
525655  130.186.6.97        192.168.1.98       TLSv1…    1222 Certificate, Server Key Exchange, Server Hello Done
528881  192.168.1.98        130.186.6.97       TCP         66 62670 → 443 [ACK] Seq=518 Ack=2697 Win=93440 Len=0 TSval=94996889 TSecr=310991

    Version: TLS 1.2 (0x0303)
    Length: 4778
  ▼ Handshake Protocol: Certificate
      Handshake Type: Certificate (11)
      Length: 4774
      Certificates Length: 4771
    ▼ Certificates (4771 bytes)
        Certificate Length: 1784
      ▶ Certificate: 308206f4308205dca003020102021055 7f1b5e9f54d5439bd21d6573f0791b300d06092a… (id-at-commonName=*.appstudenti.cineca.it,id-at
        Certificate Length: 1565
      ▶ Certificate: 3082061930820401a003020102021013 7d539caa7c31a9a433701968847a8d300d06092a… (id-at-commonName=Sectigo RSA Organization Vali
        Certificate Length: 1413
      ▶ Certificate: 30820581308204 69a00302010202103972443af922b751d7d36c10dd313595300d06092a… (id-at-commonName=USERTrust RSA Certification A

0000  c8 21 58 64 68 5b bc cf  4f 3a 0d 9d 08 00 45 00   ·!Xdh[·· O:····E·
0010  04 b8 dc 77 40 00 33 06  1b a3 82 ba 06 61 c0 a8   ···w@·3· ·····a··

Frame (1222 bytes)   Reassembled TCP (4783 bytes)

myunits-1.pcapng        Packets: 514 · Displayed: 514 (100.0%)        Profile: Default
```

Figure 4: TLS Handshake and Certificates



Certplus Root CA G2

Certificato di sicurezza

AAA Certificate Services

Rilasciato a:

Nome comune:
AAA Certificate Services

Organizzazione:
Comodo CA Limited

Unità organizzativa:

Numero di serie:
01

Rilasciato da:

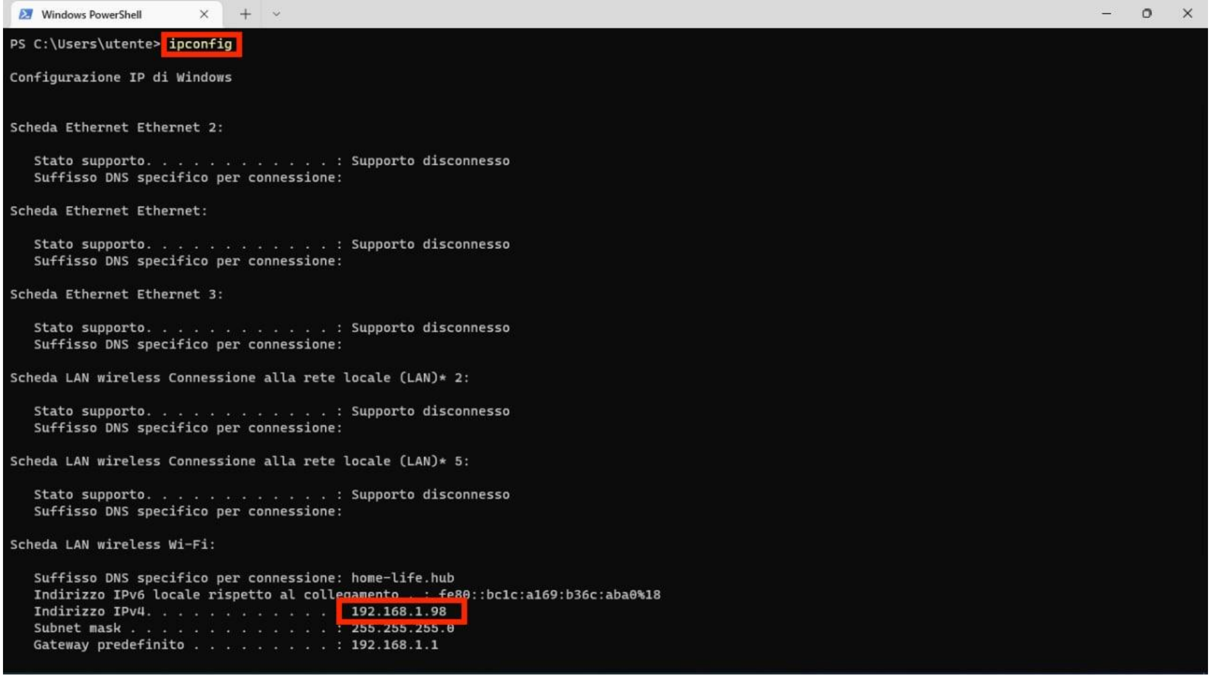
Nome comune:
AAA Certificate Services

Organizzazione:
Comodo CA Limited

Unità organizzativa:

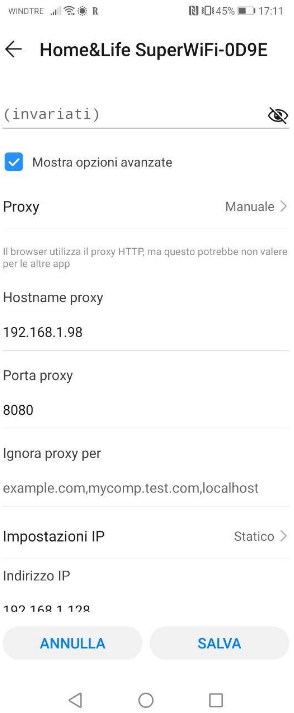
COMODO RSA Certification Authority

Figure 5: smartphone TrustSet



```
PS C:\Users\utente> ipconfig

Configurazione IP di Windows


Scheda Ethernet Ethernet 2:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:

Scheda Ethernet Ethernet:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:

Scheda Ethernet Ethernet 3:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:

Scheda LAN wireless Connessione alla rete locale (LAN)* 2:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:

Scheda LAN wireless Connessione alla rete locale (LAN)* 5:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:

Scheda LAN wireless Wi-Fi:

   Suffisso DNS specifico per connessione: home-life.hub
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::bc1c:a169:b36c:aba0%18
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.1.98
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . : 192.168.1.1
```

Figure 6: IP address of the PC



WINDTRE 45% 17:11

← Home&Life SuperWiFi-0D9E

(invariati)

☑ Mostra opzioni avanzate

Proxy Manuale >

Il browser utilizza il proxy HTTP, ma questo potrebbe non valere per le altre app

Hostname proxy

192.168.1.98

Porta proxy

8080

Ignora proxy per

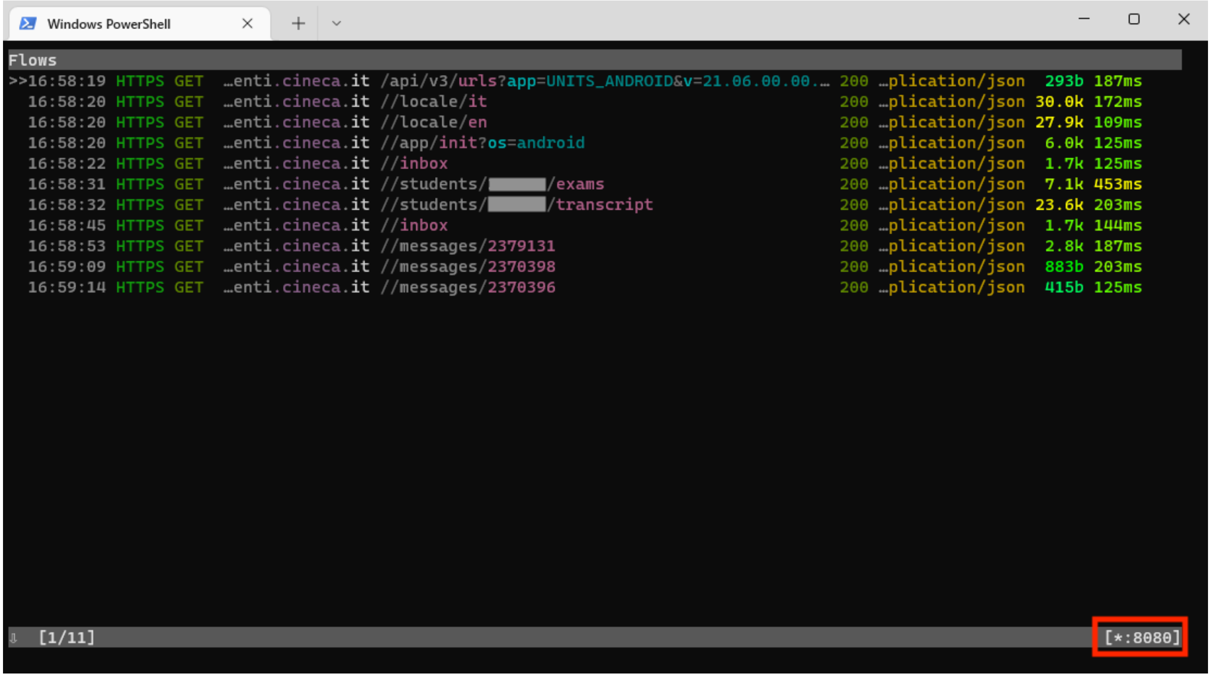
example.com,mycomp.test.com,localhost

Impostazioni IP Statico >

Indirizzo IP

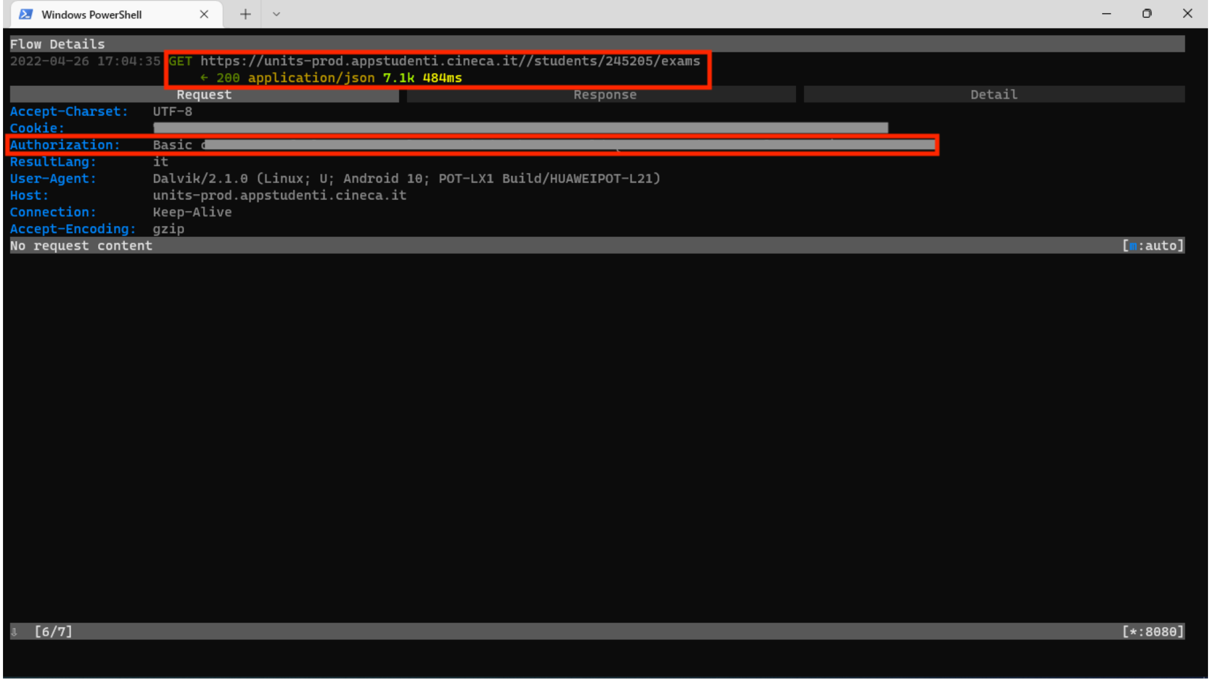
192.168.1.128

Figure 7: proxy settings



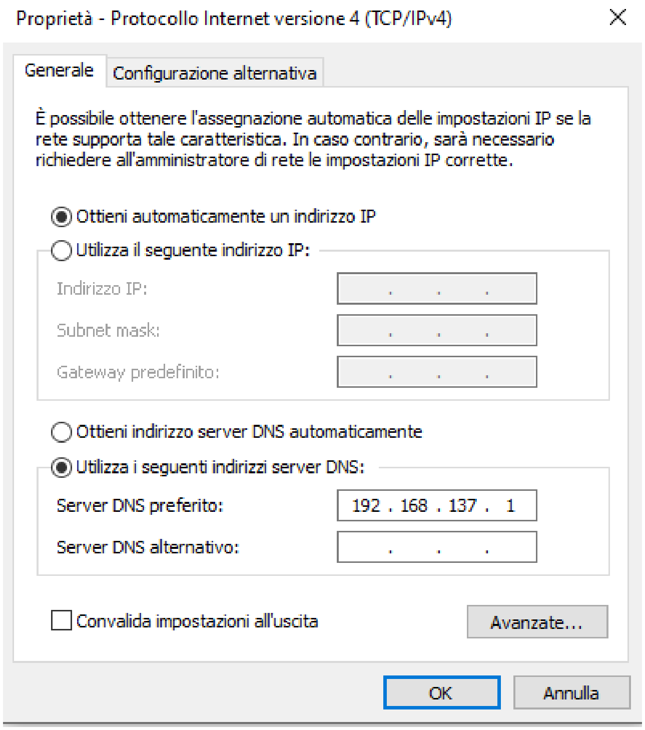
```
Flows
>>16:58:19 HTTPS GET  …enti.cineca.it /api/v3/urls?app=UNITS_ANDROID&v=21.06.00.00.… 200 …plication/json  293b 187ms
  16:58:20 HTTPS GET  …enti.cineca.it //locale/it                                    200 …plication/json 30.0k 172ms
  16:58:20 HTTPS GET  …enti.cineca.it //locale/en                                    200 …plication/json 27.9k 109ms
  16:58:20 HTTPS GET  …enti.cineca.it //app/init?os=android                          200 …plication/json  6.0k 125ms
  16:58:22 HTTPS GET  …enti.cineca.it //inbox                                        200 …plication/json  1.7k 125ms
  16:58:31 HTTPS GET  …enti.cineca.it //students/[redacted]/exams                    200 …plication/json  7.1k 453ms
  16:58:32 HTTPS GET  …enti.cineca.it //students/[redacted]/transcript               200 …plication/json 23.6k 203ms
  16:58:45 HTTPS GET  …enti.cineca.it //inbox                                        200 …plication/json  1.7k 144ms
  16:58:53 HTTPS GET  …enti.cineca.it //messages/2379131                             200 …plication/json  2.8k 187ms
  16:59:09 HTTPS GET  …enti.cineca.it //messages/2370398                             200 …plication/json  883b 203ms
  16:59:14 HTTPS GET  …enti.cineca.it //messages/2370396                             200 …plication/json  415b 125ms

⇩  [1/11]                                                                                                      [*:8080]
```

Figure 8: *mitmproxy* records



```
Flow Details
2022-04-26 17:04:35 GET https://units-prod.appstudenti.cineca.it//students/245205/exams
                        ← 200 application/json 7.1k 484ms
                    Request                         Response                        Detail
Accept-Charset:    UTF-8
Cookie:            [redacted]
Authorization:     Basic [redacted]
ResultLang:        it
User-Agent:        Dalvik/2.1.0 (Linux; U; Android 10; POT-LX1 Build/HUAWEIPOT-L21)
Host:              units-prod.appstudenti.cineca.it
Connection:        Keep-Alive
Accept-Encoding:   gzip
No request content                                                                  [m:auto]

⇩  [6/7]                                                                            [*:8080]
```

Figure 9: *mitmproxy* - HTTP GET request



Proprietà - Protocollo Internet versione 4 (TCP/IPv4)

È possibile ottenere l'assegnazione automatica delle impostazioni IP se la rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.

● Ottieni automaticamente un indirizzo IP

○ Utilizza il seguente indirizzo IP:

Indirizzo IP: . . .

Subnet mask: . . .

Gateway predefinito: . . .

○ Ottieni indirizzo server DNS automaticamente

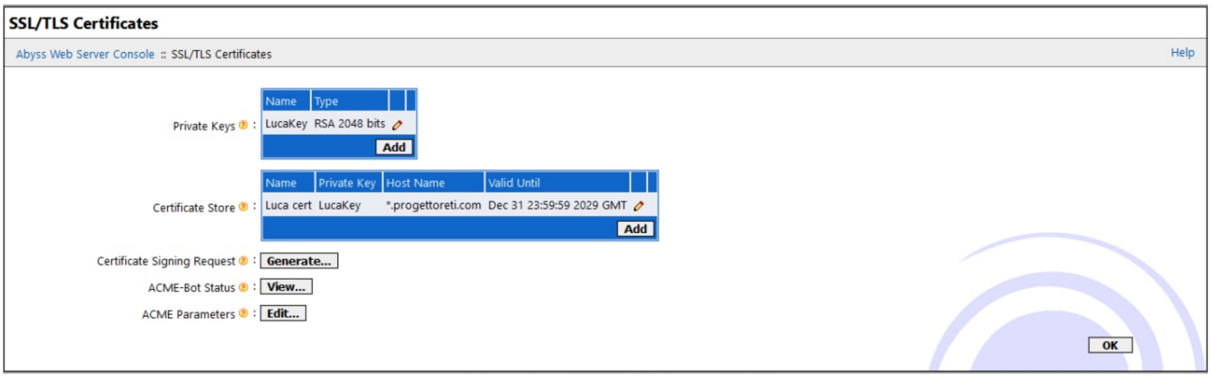
● Utilizza i seguenti indirizzi server DNS:

Server DNS preferito: 192 . 168 . 137 . 1

Server DNS alternativo: . . .

□ Convalida impostazioni all'uscita

Figure 10: Network settings



SSL/TLS Certificates

Abyss Web Server Console :: SSL/TLS Certificates

Private Keys :

Name	Type
LucaKey	RSA 2048 bits

Certificate Store :

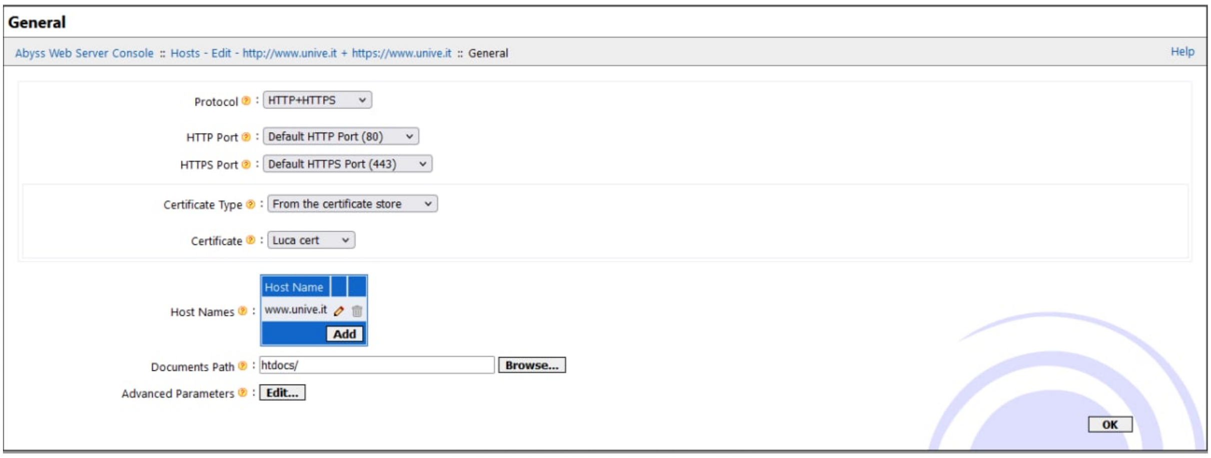
Name	Private Key	Host Name	Valid Until
Luca cert	LucaKey	*.progettoreti.com	Dec 31 23:59:59 2029 GMT

Certificate Signing Request : Generate...

ACME-Bot Status : View...

ACME Parameters : Edit...

Figure 11: SSL/TLS certificates on the *Abyss* console



General

Abyss Web Server Console :: Hosts - Edit - http://www.unive.it + https://www.unive.it :: General

Protocol : HTTP+HTTPS

HTTP Port : Default HTTP Port (80)

HTTPS Port : Default HTTPS Port (443)

Certificate Type : From the certificate store

Certificate : Luca cert

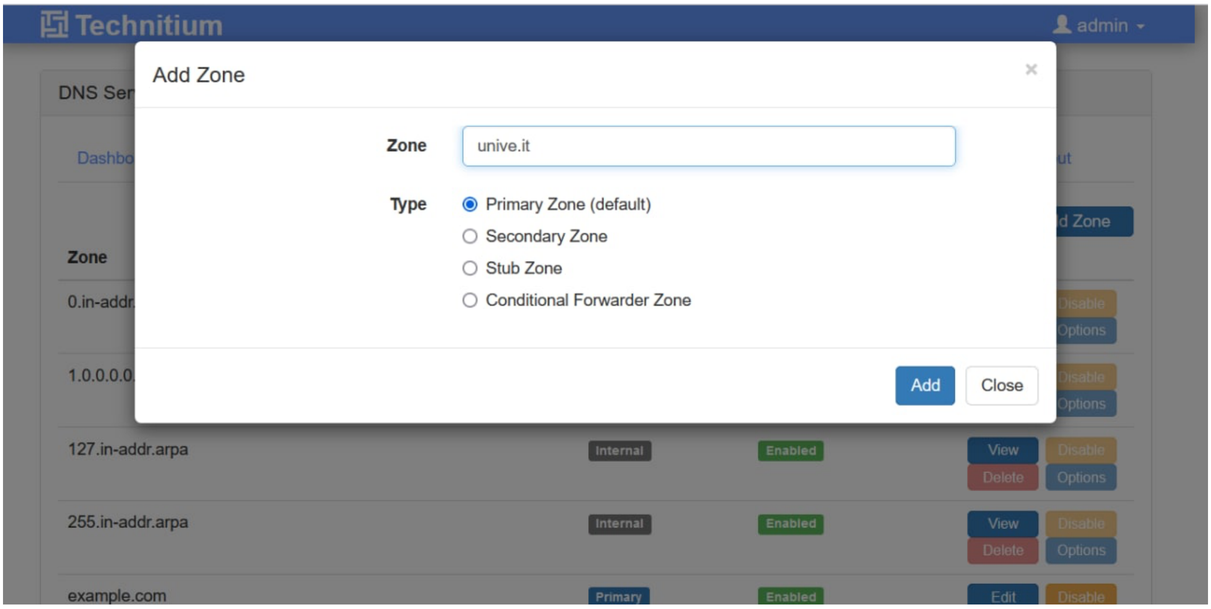
Host Names :

Host Name
www.unive.it

Documents Path : htdocs/

Advanced Parameters : Edit...

Figure 12: *Abyss* General settings



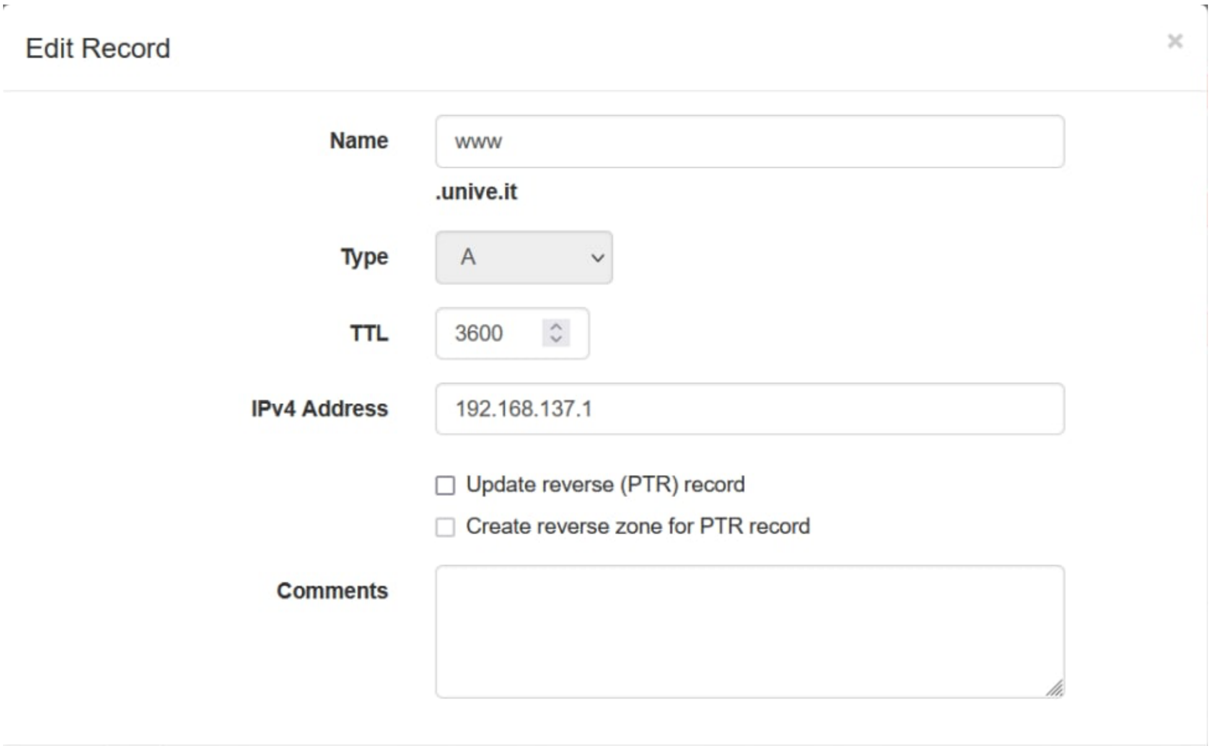
Add Zone

Zone: unive.it

Type
● Primary Zone (default)
○ Secondary Zone
○ Stub Zone
○ Conditional Forwarder Zone

Zone		
0.in-addr		
1.0.0.0.0		
127.in-addr.arpa	Internal	Enabled
255.in-addr.arpa	Internal	Enabled
example.com	Primary	Enabled

Figure 13: *Technitium* - Zone definition



Edit Record

Name: www

.unive.it

Type: A

TTL: 3600

IPv4 Address: 192.168.137.1

☐ Update reverse (PTR) record

☐ Create reverse zone for PTR record

Comments

Figure 14: *Technitium* - Record definition