WEB SERVER (Prof. Fischetti Pietro)

In informatica un server web è un'applicazione software che, in esecuzione su un server, è in grado di gestire le richieste di trasferimento di pagine web di un client, tipicamente un web browser[1]. La comunicazione tra server e client avviene tramite il protocollo HTTP, che utilizza la porta TCP di default 80 (o 8080), o eventualmente la versione sicura HTTPS, che utilizza invece di default la 443. Su un server web risiedono dunque i siti web tramite hosting. L'insieme di tutti i server web interconnessi a livello mondiale dà vita al World Wide Web.

XAMPP (windows)

Il pacchetto Xampp (nel proseguio si ipotizza che sia stato caricato nella directory c:\xampp) per windows (portabile quindi gestibile e configurabile anche se non si e' amministratori) contiene tra le altre cose il web server Apache portato dal mondo Linux nel mondo Windows.

Come prima cosa si controlli le porte disponibili con il comando netstat –n in modo da configurare oppotunamente apache utilizzando eventualmente altre porte se quella http 80 https 443 sono occupate (si ricorda che non puo' esserci piu' di un servizio in ascolto su una porta).

I siti devono essere memorizzati nella cartella: C:\xampp\htdocs come sottocartelle, ad esempio se voglio un sito che chiamo mySite che contiene semplicemente un file il cui contenuto e':ciao

il file puo' avere qualsiasi nome ma se si chiama index.html verra presentato di defaut quando viene richiesto dal bowser:http://localhost/mysite non server <u>http://localhost/mysite/index.html</u>, mentre se volessi un altro file devo specificarlo ad es <u>http://localhost/mysite/pagina2.html</u> ma anche <u>http://localhost/mysite/es.txt</u>. Questi sono file statici ma sevoglio rendere le risposte dinamiche cioe' dipendenti da qualche parametro passato dal browser posso usare il linguaggio PHP. in pratica viene eseguito del codice lato server racchiuso da dei tag speciali. Se il Web Server e' correttamente configurato ad esempio:

8	XAN	MPP Contr	ol Panel v3	.2.2				J Co	onfig
Modules Service	Module	PID(s)	Port(s)	Actions				🙆 Ne	tstat
	Apache	2484 7248	80, 443	Stop	Admin	Config	Logs	S 🔤	hell
	MySQL	8636	3306	Stop	Admin	Config	Logs	Expl	olorer
	FileZilla			Start	Admin	Config	Logs	🛃 Ser	vices
	Mercury			Start	Admin	Config	Logs	O H	lelp
	Tomcat			Start	Admin	Config	Logs		Quit
2:42:54	[main]	XAMPP In:	stallation Direct	ory: "c:\xan	npp\"				
2:42:54	[main]	Checking f	or prerequisites						
2:42:56	[main]	All prerequ	isites found						
2:42:56	[main]	Initializing	Modules						
2:42:56	[Apache]	XAMPP A	bache is already	running on	port 443				- 1
2:42:56	[mysql]	XAMPP M	ySQL is already	y running on	port 3306				
2.42.56	[main]	Starting Ch	neck-Timer						
2.12.00		Control Do	nal Dandur						

Ma nel caso il server http dalla porta 80 si potrebbe ad esempio spostare sulla porta 8080 (ovvio se libera altrimenti si cerchi una libera) modificando il file httpd.conf attivabile dal bottone Config, e cercando la linea: Listen 80

XAMPP Contr	ol Panel v3.2.2 [Co	mpiled: Nov 12th 2	2015]				<u> (11</u>)		×
8	XAMPP Cont	Config							
Service Mode	ile PID(s)	Netstat							
Apac	he 15712 15776	443, <mark>80</mark> 80	Shell						
MySt	2L 14544	Explorer							
FileZ	illa Start Admin Config Logs								
Merc	iry		Start	Admin	Config	Logs	😢 Help		
Tomo	at		Start	Admin	Config	Logs	Quit		
10:41:44 [main] Initializing Control Panel 10:41:44 [main] Windows Version: Enterprise 64-bit 10:41:44 [main] XAMPP Version: 7.2.12 10:41:44 [main] Control Panel Version: 3.2.2 [Compiled: Nov 12th 2015] 10:41:44 [main] You are not running with administrator rights! This will work for 10:41:44 [main] most application stuff but whenever you do something with services 10:41:44 [main] there will be a security dialogue or things will break! So think 10:41:44 [main] about running this application with administrator rights! 10:41:44 [main] about running this application with administrator rights! 10:41:44 [main] AMPP Installation Directory: "c:\xampb\" 10:41:44 [main] Checking for prerequisites 10:41:46 [main] All prerequisites found 10:41:46 [main] Initializing Modules 10:41:46 [main] Starting Check-Timer 10:41:46 [main] Control Panel Ready 10:42:28 [Apache] Attempting to stop Apache (PID: 15028) 10:42:28 [Apache] Status change detected: stopped									

In questo caso digitando nel browser: http://localhost:8080 dovrebbe apparire la pagina splash di Apache



Vediamo ora coe creare un proprio sito ad esempio di nome mySite-

Creare il percorso: c:\xampp\htdocs\mySite

E creareci un file index.html

che contiene semplicemente la parola ciao:

index.html	
ciao	

Digitare nel browser:



ciao

Vediamo come passare dei parametri dal browser ad un nostro programma (che chiamo ad esempio Index.php) in esecuzione sul Web Server. I metodi maggiormente utilizzati sono GET e POST. Con il metodo GET i parametri possono inserirli direttamente nella barra come coppie nome=valore separate dal carattere &. Quindi mettiamo nella dir mySite il file:



Digitiamo nel browser: http://localhost/mySite/?nome=pedro&city=siviglia



Questo avviene perche l'url viene passato nella query string del server:

modificando il file index.php:

```
Index.php
<?php
print "ola " . $_GET["nome"] . " da " . $_GET["city"];
echo "";
print_r($_SERVER);
echo "";
?>
```

Posso vedere nel dettaglio le stringhe configurate dal Web Server per il mio codice php.

← → C ③ localhost/mySite/?nome=pedro&city=siviglia

ola pedro da siviglia

.

```
Array
     [MIBDIRS] => C:/xampp/php/extras/mibs
     [MYSQL_HOME] => \xampp\mysql\bin
     [OPENSSL_CONF] => C:/xampp/apache/bin/openssl.cnf
     [PHP_PEAR_SYSCONF_DIR] => \xampp\php
     [PHPRC] => \xampp\php
     [TMP] => \xampp\tmp
[HTTP_HOST] => localhost
     [HTTP_CONNECTION] => localHOST
[HTTP_CONNECTION] => keep-alive
[HTTP_CACHE_CONTROL] => max-age=0
[HTTP_SEC_CH_UA] => "Google Chrome";v="111", "Not(A:Brand";v="8", "Chromium";v="111")
[HTTP_SEC_CH_UA] => "Google Chrome";v="111", "Not(A:Brand";v="8", "Chromium";v="111")
     [HTTP_SEC_CH_UA_MOBILE] => ?0
     [HTTP_SEC_CH_UA_PLATFORM] => "Windows"
     [HTTP_UPGRADE_INSECURE_REQUESTS] => 1
     [HTTP_USER_AGENT] => Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, 1:
     [HTTP_ACCEPT] => text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web;
     [HTTP_SEC_FETCH_SITE] => none
     [HTTP_SEC_FETCH_MODE] => navigate
     [HTTP_SEC_FETCH_USER] => ?1
     [HTTP_SEC_FETCH_DEST] => document
     [HTTP_ACCEPT_ENCODING] => gzip, deflate, br
[HTTP_ACCEPT_LANGUAGE] => it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
     [HTTP_COOKIE] => PHPSESSID=r4iu842so6s334sqe88504ad72
     [PATH] => C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\Window
     [SystemRoot] => C:\Windows
     [COMSPEC] => C:\Windows\system32\cmd.exe
     [PATHEXT] => .COM; .EXE; .BAT; .CMD; .VBS; .VBE; .JS; .JSE; .WSF; .WSH; .MSC
     [WINDIR] => C:\Windows
     [SERVER_SIGNATURE] =>
Apache/2.4.28 (Win32) OpenSSL/1.0.2L PHP/7.1.10 Server at Localhost Port 80
     [SERVER_SOFTWARE] => Apache/2.4.28 (Win32) OpenSSL/1.0.21 PHP/7.1.10
     [SERVER_NAME] => localhost
     [SERVER_ADDR] => ::1
      SERVER_PORT] => 80
     [REMOTE_ADDR] => ::1
     [DOCUMENT_ROOT] => C:/xampp/htdocs
     [REQUEST_SCHEME] => http
[CONTEXT_PREFIX] =>
     [CONTEXT_DOCUMENT_ROOT] => C:/xampp/htdocs
     [SERVER_ADMIN] => postmasten@localhost
     [SCRIPT_FILENAME] => C:/xampp/htdocs/mySite/index.php
[REMOTE_PORT] => 60106
     [GATEWAY_INTERFACE] => CGI/1.1
[SERVER_PROTOCOL] => HTTP/1.1
     [REQUEST_METHOD] => GET
     [QUERY_STRING] => nome=pedro&city=siviglia
     [REQUEST_URI] => /mySite/?nome=pedro&city=siviglia
[SCRIPT_NAME] => /mySite/index.php
      PHP_SELF] => /mySite/index.php
     [REQUEST_TIME_FLOAT] => 1679498446.721
     [REQUEST_TIME] => 1679498446
)
```

Si veda il valore [QUERY_STRING] che contiene le coppie nome=valore

Vediamo ora di utilizzare un file html con richiesta GET:

```
esGETPOST.html

<!DOCTYPE html>

<html>

<body>

<form action="http://localhost/mySite/my.php" method="GET">

<label for="nome">name:</label>

<label for="nome">name:</label>

<input type="text" id="nome" name="nome"><br><br><label for="city">city:</label>

<input type="text" id="city" name="city"><br><br>
```

<input <="" th="" type="submit"/> <th>value="Submit"></th>	value="Submit">

</body> </html>

Inoltre aggiungiamo nel file index.php la gestione del case GET o POST

Index.php
php</td
print "ola ";
if(\$_SERVER['REQUEST_METHOD']=="GET"){
if(isset(\$_GET["nome"]))
print \$_GET["nome"];
if(isset(\$_GET["city"]))
print " da " . \$_GET["city"];
}
elseif(\$_SERVER['REQUEST_METHOD']=="POST"){
if(isset(\$_POST["nome"]))
print \$_POST["nome"];
if(isset(\$_POST["city"]))
print " da " . \$_POST["city"];
}
echo " <pre>";</pre>
print_r(\$_SERVER);
echo "";
?>

S esGETPOST.html	× +	
\leftrightarrow \rightarrow C (1) Archi	vio C:/esGETPOST.html	
name: pedro		
city: siviglia		
Submit		

```
Iocalhost/mySite/r
                            ×
                                +
    → C ① localhost/mySite/?nome=pedro&city=siviglia
ola pedro
Array
(
   [MIBDIRS] => C:/xampp/php/extras/mibs
   [MYSQL_HOME] => \xampp\mysql\bin
   [OPENSSL_CONF] => C:/xampp/apache/bin/openssl.cnf
   [PHP_PEAR_SYSCONF_DIR] => \xampp\php
   [PHPRC] => \xampp\php
   [TMP] => \xampp\tmp
   [HTTP_HOST] => localhost
    .....
    .....
```

```
[CONTEXT_DOCUMENT_ROOT] => C:/xampp/htdocs
[SERVER_ADMIN] => postmaster@localhost
[SCRIPT_FILENAME] => C:/xampp/htdocs/mySite/my.php
[REMOTE_PORT] => 51622
[GATEWAY_INTERFACE] => CGI/1.1
[SERVER_PROTOCOL] => HTTP/1.1
[REQUEST_METHOD] => GET
[QUERY_STRING] => nome=pedro&city=siviglia
[REQUEST_URI] => /mySite/my.php?nome=pedro&city=siviglia
[SCRIPT_NAME] => /mySite/my.php
```

Nel metodo POST i parametri non vengono trasmessi nell'url come coppie. Ma sono inseriti nel corpo della richiesta, quindi non sono visibili e possono superare le limitazioni in lunghezza dell'URL presenti nel metodo GET (max 2048 caratteri)

```
esGETPOST.html

<!DOCTYPE html>

<html>

<body>

<form action="http://localhost/mySite/index.php" method="POST">

<label for="nome">name:</label>

<input type="text" id="nome" name="nome"><br><br><

<label for="city">city:</label>

<input type="text" id="city" name="city"><br>>

<input type="text" id="city" name="city"><br>>

<input type="submit" value="Submit">

</form>

</body>

</html>
```

← → C () localhost/mySite/mySite/index.php

```
ola pedro da siviglia
```

```
Array
(
    [MIBDIRS] => C:/xampp/php/extras/mibs
    [MYSQL_HOME] => \xampp\mysql\bin
    [OPENSSL_CONF] => C:/xampp/apache/bin/openssl.cnf
    [PHP_PEAR_SYSCONF_DIR] => \xampp\php
    [PHPRC] => \xampp\php
    [TMP] => \xampp\tmp
    [HTTP_HOST] => localhost
    ......
    .....
    [CONTEXT_DOCUMENT_ROOT] => C:/xampp/htdocs
    [SERVER_ADMIN] => postmaster@localhost
    [SCRIPT_FILENAME] => C:/xampp/htdocs/mySite/my.php
    [REMOTE_PORT] => 51634
    [GATEWAY_INTERFACE] => CGI/1.1
    [SERVER_PROTOCOL] => HTTP/1.1
    [REQUEST_METHOD] => POST
    [QUERY_STRING] =>
    [REQUEST_URI] => /mySite/my.php
    [SCRIPT_NAME] => /mySite/my.php
    [PHP_SELF] => /mySite/my.php
                               ----
```

Si nota che sono sparite le coppie nome=valore dalla barra URL del browser. Si potrebbe controllare per esercizio il traffico Request-Response tramite Ispezione dal Browser o con Wireshark, oppure con Fiddler.



Nella figura seguente la risposta ad una richiesta https di tipo GET:

Mttps://192.168.1.53/mySite/?non × +
 ← → C ▲ Non sicuro | https://192.168.1.53/mySite/?nome=pedro&city=siviglia

```
ola pedro da siviglia
```

Array

```
(
    [MIBDIRS] => C:/xampp/php/extras/mibs
    [MYSQL_HOME] => \xampp\mysql\bin
    [OPENSSL_CONF] => C:/xampp/apache/bin/openssl.cnf
    [PHP_PEAR_SYSCONF_DIR] => \xampp\php
    [PHPRC] => \xampp\php
    [TMP] => \xampp\tmp
    [HTTPS] => on
    [SSL_SERVER_S_DN_C] => IT
    [SSL_SERVER_S_DN_ST] => Italy
    [SSL_SERVER_S_DN_L] => Genova
    [SSL_SERVER_S_DN_0] => acme
    [SSL_SERVER_S_DN_OU] => cpp
    [SSL_SERVER_S_DN_CN] => mysite.dev
    [SSL_SERVER_S_DN_Email] => my@acme.it
    [SSL_SERVER_I_DN_C] => IT
    [SSL_SERVER_I_DN_ST] => Italy
    [SSL_SERVER_I_DN_L] => Genova
    [SSL_SERVER_I_DN_0] => acme
    [SSL_SERVER_I_DN_OU] => cpp
    [SSL_SERVER_I_DN_CN] => mysite.dev
    [SSL_SERVER_I_DN_Email] => my@acme.it
    [SSL_VERSION_INTERFACE] => mod_ssl/2.4.28
    [SSL VERSION LIBRARY] => OpenSSL/1.0.21
    [SSI PROTOCOL1 => TLSv1.2
```

Nella figura seguete la cattura del traffico con Fiddler

Headers	TextView	WebForms	HexView	Auth Raw	XML									
CONNECT Host: 19 Proxy-Co User-Age	192.168.1 2.168.1.5 nnection: nt: Mozil	.53:443 HTT 3:443 keep-alive la/5.0 (Win	P/1.1 dows NT 10.	.0; <mark>W</mark> in64;	x64) Ap	oplewebKi	t/537.36	(KHTML	, like G	iecko) C	hrome/	111.0.0	.0 Safari/	37.36
The data	sent rep	resents a S	SLv3-compat	tible Clien	tHello	handshak	e. For y	our co	nvenienc	e, the	data i	s extra	cted below	
Major Ve Minor Ve Random: SessionI Ciphers:	rsion: 3 rsion: 3 BF 4F 85 D: 78 63 1301] Unr 1302] Unr 1302] Unr 0228] Unr C028] Unr C026] Unr C026] Unr C026] Unr C026] Unr C030] Unr	66 BB 90 3A 70 F9 D2 25 ecognized c ecognized c ecognized c ecognized c ecognized c ecognized c ecognized c ecognized c L_CK_ECDHE_ ecognized c ecognized c ecognized c	FF AE 19 (04 01 EF 4 ipher ipher ipher ipher ipher ipher ipher sA_WITH_AE sSA_WITH_AE ipher ipher sSA_WITH_AE	C8 D8 CF 6C 41 16 9D 24 55_128_C8C_ 55_256_C8C_	SHA SHA	6C D5 7C D6 72 26	DD FF A4 D2 78 35	4 8E 4E EO FO	AG CA C 58 B8 E	8 7C 74	9B DA FD D3	00 59 57		
Hex	Find	N34_463_23	0_344											
Transforme	r Heade	rs TextView	/ ImageView	HexView	Auth	Caching	Privacy	Raw	XML					
HTTP/1.1 Timestam	200 Conn p: 09:30:	ection Esta 51:0420	blished		1	1	1	Tran		1				
This is To view id=rpasp The data Major Ve Minor Ve SessionI Random: Cipher:	a CONNECT the header sent repr rsion: 3 D: empty DE AS CS 0xC030	tunnel, th rs of the e resents a S 16 D5 00 38	rough which ncrypted W SLv3-compat	h encrypted inINET traf tible Serve CO EB A2 62	HTTPS fic ins rHello PF9 EA	traffic side this handshak OD 3A FD	flows. tunnel, e. For y 7E 7F 82	instal vour con 2 9E 67	l the RP nvenienc A2 B5 3	ASpy pl e, the 8 2D 16	ugin fi data i B6 C5	rom <u>htt</u> s extra B4	<u>o://www.fi</u>	<u>ddlerto</u>

CGI

In informatica Common Gateway Interface (CGI) è una tecnologia standard usata dai web server per interfacciarsi con applicazioni esterne generando contenuti web dinamici. In pratica possiamo utilizzare dei programmi eseguibili ad esempio scritti in C per essere richiamti dal Web Server. Esempio: un programma C che calcoli la somma di 2 numeri:

```
cgisum.c
#include <stdio.h>
#include <stdlib.h>
int main(int argc, char **argv, char** env) {
int n1=0,n2=0,r;
char *data = getenv("QUERY_STRING");
r=sscanf(data,"number1=%d&number2=%d",&n1,&n2);
printf("Content-type: text/html\n\n");
printf("<html><head><title>CGI C Example</title></head>\n");
printf("<body><h1>CGI C Example</h1>\n");
if(r!=2)
{
printf("Input data error\n");
}
else
{
 printf("%d + %d = %d<br><br>",n1,n2,n1+n2);
```

}
//Vogliamo stampare le varibili d'ambiente per curiosita'
while (*env)
 printf("
%s", *env++);
printf("</body></html>\n");
return 0;
}

Naturalmente il programma deve essere richiamto da un server e l'input non arriva normalmente da tastiera ma dalle variabili d'ambiente che possono essere lette dalla funzione getenv(). Inoltre si e' modificato la scrittura tramite printf per restituire un samplice pagina html con alcuni tag.

Poi creiamo un sito ed esempio:C:\xampp\htdocs\mycgi

con la seguente pagina

Index.html
<html></html>
<head></head>
<title>my CGI Example</title>
<body></body>
<form action="/cgi-bin/cgisum.exe" method="get"></form>
Enter first number <input name="number1" type="text"/>
Enter second number <input name="number2" type="text"/>
<input type="submit" value="Calculate sum"/>

my CGI Example	×	+
\leftrightarrow \rightarrow C (localhost/mycgi/	
Enter first number	3	
Enter second num	ber 2	
Calculate sum		

← → C (i) localhost/cgi-bin/cgisum.exe?number1=3&number2=2

CGI C Example

3 + 2 = 5

MIBDIRS=C:/xampp/php/extras/mibs MYSQL_HOME=xampp/inpysql/bin OPENSSL_CONF=C:/xampp/apache/bin/opensal.cnf PHP_PEAR_SYSCONF_DIR=/xampp/php TMP=/xampp/tmp HTTP_HOST=localhost HTTP_CONNECTION=kcep-alive HTTP_SEC_CH_UA="Google Chrome";v="111", "Not(A:Brand";v="8", "Chromium";v="111" HTTP_SEC_CH_UA_FLORM="Windows" HTTP_SEC_CH_UA_PLATFORM="Windows" HTTP_USER_AGENT=Mozilla'5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chron HTTP_JOST_ADE_INSECURE_REQUESTS=1 HTTP_USER_AGENT=Mozilla'5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chron HTTP_ACCEPT=text/html,application/khtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apig,*/*;q=0.8,a HTTP_SEC_FETCH_SITE=same-origin HTTP_SEC_FETCH_USER=?1 HTTP_SEC_FETCH_USER=?1 HTTP_SEC_FETCH_USER=?1 HTTP_ACCEPT_LANGUAGE=it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7 PATH=C:Windows!system32;C:Windows:System32;Wbem;C:Windows:Apps;C:Users\FP\.dotnet'toc SystemRoot=C:Windows SystemRoot=C:Windows SystemS2:Cumdows COMSPEC=C:Windows SystemS2:Cumdows'system32;Cimd.exe PATHEXT=COM;EXE_BAT;CMD;VBS;VBE;JS;JSE;.WSF;WSH;MSC WINDIR=C:Windows SERVER_SIGNATURE= Apache/2.4.28 (Win32) OpenSSL/1.0.21 PHP/7.1.10 Server at localhost Port 80 SERVER_SOFTWARE=Apache/2.4.28 (Win32) OpenSSL/1.0.21 PHP/7.1.10

SERVER_SOFTWARE=Apache/2.4.28 (Win32) OpenSSL/1.0.21 PHP/7.1.10 SERVER_NAME=localhost SERVER_ADDR=::1 SERVER_ADDR=::1 DOCUMENT_ROOT=C:/xampp/htdocs REQUEST_SCHEME=http CONTEXT_PREFIX=/cgi-bin/ CONTEXT_PREFIX=/cgi-bin/ SERVER_ADMIN=postmaster@localhost SCRIPT_FILENAME=C:/xampp/cgi-bin/cgisum.exe REMOTE_PORT=51684 GATEWAY_INTERFACE=CGI/1.1 SERVER_PROTOCOL=HTTP/1.1 REQUEST_METHOD=GET QUERY_STRING=number1=3&number2=2 REQUEST_URI=/cgi-bin/cgisum.exe

HTTPS

XAMPP Control Panel v3.2.2 Modules Module PID(s) Port(s) Actions Apache 2484 80,443 Stop Admin Config MySQL 8636 3306 Stop Admin Con Apache (httpd.conf) MySQL 8636 3306 Stop Admin Con Apache (httpd.conf) Mercury Start Admin Con PHP (php.ini) PhpMyAdmin (config.inc.php) 12:42:54 [main] Checking for prerequisites Start Admin Con 12:42:56 [main] All prerequisites found Initializing Modules Starting Check-Timer 12:42:56 [main] Starting Check-Timer Control Panel Ready Starting Check-Timer	🔀 XAMP	P Control Par	nel v3.2.2 [Com	npiled: Nov 12th 2	2015]			1		×	
Service Module PID(s) Port(s) Actions Apache 2484 7248 80, 443 Stop Admin Confia Loos Shell MySQL 8636 3306 Stop Admin Con Apache (httpd.conf) MySQL 8636 3306 Stop Admin Con Apache (httpd.conf) Mercury Start Admin Con Apache (httpd-ssl.conf) Mercury Start Admin Con Tomcat Start Admin Con 12:42:54 [main] XAMPP Installation Directory: "c:\xampp\" <browse> [Apache] 12:42:56 [main] All prerequisites found Browse> [PHP] 12:42:56 [main] Initializing Modules Browse> [phpMyAdmin] 12:42:56 [main] Starting Check-Timer Control Panel Ready 12:42:56 [main] Starting Check-Timer Control Panel Ready</browse>	8	XAN	MPP Contr	ol Panel v3	.2.2				de ca	onfig	
Apache 2484 7248 80, 443 Stop Admin Confia Loos Shell MySQL 8636 3306 Stop Admin Con Apache (httpd.conf) FileZilla Start Admin Con Apache (httpd.ssl.conf) Apache (httpd-ssl.conf) Mercury Start Admin Con Apache (httpd-ssl.conf) Mercury Start Admin Con PHP (php.ini) Tomcat Start Admin Con Story 12:42:54 (main) Checking for prerequisites Story Story Story 12:42:56 (main) All prerequisites found Story Story Story Story 12:42:56 [main] Initializing Modules Starting Check-Timer Story Story Story 12:42:56 [main] Starting Check-Timer Control Panel Ready Story Story Story 12:42:56 [main] Control Panel Ready Story Story Story Story	Service	Module	PID(s)	Port(s)	Actions				🥑 Ne	etstat	
MySQL 8636 3306 Stop Admin Con FileZilla Start Admin Con Apache (httpd-ssl.conf) Mercury Start Admin Con Morcury Start Admin Con Tomcat Start Admin Con 12:42:54 [main] Checking for prerequisites All prerequisites found 12:42:56 [main] Initializing Modules 12:42:56 [main] Initializing Modules 12:42:56 [main] Starting Check-Timer Control Panel Ready		Apache	2484 7248	80, 443	Stop	Admin	Confia	Loos	P 5	Shell	
FileZilla Start Admin Con Mercury Start Admin Con Tomcat Start Admin Con 12:42:54 [main] XAMPP Installation Directory: "c:\xampp\" PHP (php.ini) 12:42:54 [main] XAMPP Installation Directory: "c:\xampp\" Start 12:42:54 [main] Checking for prerequisites Start 12:42:56 [main] All prerequisites found Start 12:42:56 [main] Initializing Modules Starting Check-Timer 12:42:56 [main] Starting Check-Timer Starting Check-Timer 12:42:56 [main] Control Panel Ready Maption port 3306		MySQL	8636	3306	Stop	Admin	Con	Apache (http	od.conf)	.0	
Mercury Start Admin Con Tomcat Start Admin Con 12:42:54 [main] XAMPP Installation Directory: "c:\xampp\" <browse> [Apache] 12:42:54 [main] Checking for prerequisites <browse> [PHP] 12:42:56 [main] All prerequisites found <browse> [PHP] 12:42:56 [main] Initializing Modules <browse> [phpMyAdmin] 12:42:56 [Apache] XAMPP Apache is already running on port 443 12:42:56 [msin] Starting Check-Timer 12:42:56 [main] Starting Check-Timer 12:42:56 [main] Control Panel Ready</browse></browse></browse></browse>		FileZilla			Start	Admin	Con	Apache (http	od-ssi.cor	n) p.conf)	
Tomcat Start Admin Con phpMyAdmin (config.inc.php) 12:42:54 [main] XAMPP Installation Directory: "c:\xampp\" <browse> [Apache] 12:42:54 [main] Checking for prerequisites <browse> [PHP] 12:42:56 [main] Initializing Modules <browse> [phpMyAdmin] 12:42:56 [Main] Initializing Modules <browse> [phpMyAdmin] 12:42:56 [Apache] XAMPP Apache is already running on port 443 12:42:56 [main] Starting Check-Timer Starting Check-Timer 12:42:56 [main] Control Panel Ready With the starting Check-Timer</browse></browse></browse></browse>		Mercury			Start	Admin	Con	PHP (php.in	PHP (php.ini)		
12:42:54 [main] XAMPP Installation Directory: "c:\xampp\" <browse> [Apache] 12:42:54 [main] Checking for prerequisites <browse> [PHP] 12:42:56 [main] All prerequisites found <browse> [phpMyAdmin] 12:42:56 [main] Initializing Modules <browse> [phpMyAdmin] 12:42:56 [mysql] XAMPP Apache is already running on port 443 12:42:56 [mysql] XAMPP MySQL is already running on port 3306 12:42:56 [main] Starting Check-Timer 12:42:56 [main] Control Panel Ready</browse></browse></browse></browse>		Tomcat			Start	Admin	Con	phpMyAdm	in (config	.inc.php))
· · · · · · · · · · · · · · · · · · ·	12:42:54 12:42:54 12:42:56 12:42:56 12:42:56 12:42:56 12:42:56 12:42:56	Tomcat Start Admin Con priprivyAdmin 12:42:54 [main] XAMPP Installation Directory: "c:\xampp\" <browse> [12:42:54 [main] Checking for prerequisites <browse> [12:42:56 [main] All prerequisites found <browse> [12:42:56 [main] Initializing Modules 12:42:56 [Apache] XAMPP Apache is already running on port 443 12:42:56 [mysql] XAMPP MySQL is already running on port 3306 12:42:56 [main] Starting Check-Timer 12:42:56 [main] Control Panel Ready</browse></browse></browse>									

Per configurare Apache affinche risponda a richieste HTTPS, avviare il programma

c:\xampp\apache\makecert.bat



Una volta terminato vengono create i file:

il certificato:

C:\xampp\apache\conf\ssl.crt\server.crt

Ela chiave privata:

C:\xampp\apache\conf\ssl.key\server.key

Il file che regola HTTPS o meglio SSL si trova in:

C:\xampp\apache\conf\extra\httpd-ssl.conf

Qui si trova la riga:

Listen 443

Che dice su quale porta apache ascolta le richieste https

Mentre la riga:

SSLCertificateFile "conf/ssl.crt/server.crt"

Indica il certificato utilizzato da apache per soddisfare le richieste https.

Infine:

.....

<VirtualHost _default_:443>

General setup for the virtual host DocumentRoot "C:/xampp/htdocs"

Indica il percorso che apache proteggera'.

Il certificato prodotto in precednza con makecert e' autogenerato infatti possiamo verificarlo con il comando:

C:\xampp\apache\bin> openssl s_client -showcerts -connect localhost:443

o ALPN negotiated
SL-Session:
Protocol : TLSv1.2
Cipher : ECDHE-RSA-AES256-GCM-SHA384
Session-ID: C36E032C83ADC7EFB11E73E8A268B80746D4C4A35573F8A29831469D5FE875CF
Session-ID-ctx:
Master-Key: CD3491D9E94B82CD6784F05EE71C42E3DABB494F58AD26138338733CD20A192320494C78F2
Key-Arg : None
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 300 (seconds)
TLS session ticket:
0000 - 7e fc 18 4b b5 87 4d 8d-5e 01 45 53 62 b4 94 b4 ~KM.^.ESb
0010 - 5c 78 3d 4e 53 d2 4f 60-2d 3d df b2 42 9f b0 e6 \x=NS.O`-=B
0020 - 9a 43 59 60 6d fb 69 a0-30 60 d2 77 1e 93 06 7f .CY`m.i.O`.w
0030 - a4 4a d1 25 10 1d 81 fd-e5 43 35 0d 33 1e 0b d4 .J.%C5.3
0040 - e5 3a 2a 78 b8 75 e3 2d-9e a7 68 59 13 f1 37 53 .:*x.uhY7S
0050 - 0c 9b 6c 2a fe 48 d5 b8-98 af 0e c4 97 3f 18 3el*.H?.>
0060 - a9 4e eb 2c d7 5d d4 cd-b6 e5 a1 88 cd 32 0b 1f .N.,.]2
0070 - e1 c8 4b 6b 10 a6 03 70-cc 2c d6 d9 98 2b 89 e8Kkp.,+
0080 - 3d 75 55 72 cb 9b 50 ea-be f6 7a 1c 79 d7 68 01 =uUrPz.y.h.
0090 - ba 0e 8d cc 04 2b 58 cb-93 74 45 02 e7 8a d6 52+XtER
00a0 - b3 39 a3 31 2e 5d 09 99-08 bd 49 f2 e7 ad 87 22 .9.1.]I"
00b0 - 45 8b 77 27 93 90 85 f6-d7 73 5c 3d e2 f0 eb 69 E.w's\=i
Start Time: 1679489106
Timeout : 300 (sec)
Verify return code: 18 (self signed certificate)

Dove nell'ultima riga dice che il certificato e' effettivamete autogenerato.

Ora se avvio la richiesta:

https://localhost

Ottengo:



Se si vuole evitare che chrome non visualizzi il messaggio precedente:

chrome://flags/#allow-insecure-localhost e abilitare la voce:

Allow invalid certificates for resources loaded from localhost

Il Web Server Microsoft Internet Inforation Services (IIS)[CENNI].

Puo' essere installato, se si e' amministratori, tramite le "Funzionalita' di Windows" dal Pannello di controllo.

🔤 Funzionalità Windows —		×
Attivazione o disattivazione delle funzionalità Windows		8
Per attivare una funzionalità, selezionare la relativa casella di controllo. Per deselezionare la relativa casella di controllo. Una casella piena indica che è parte della funzionalità.	r disattiv è attivata	arla, solo
HWC (Hostable Web Core) di Internet Information Services		^
⊕ Hyper-V		
IFilter TIFF di Windows		
Internet Explorer 11		
🖃 🔳 🔄 Internet Information Services		
🗄 🔳 🔄 Server FTP		
🖃 🔳 🔄 Servizi Web		
🕀 🔳 📙 Funzionalità HTTP comuni		
🕀 🔳 📕 Funzionalità per lo sviluppo di applicazioni		
🕀 🔳 📕 Funzionalità prestazioni		
🕀 🔳 📙 Integrità e diagnostica		
🕀 🔳 📑 Sicurezza		
🕀 🔳 🔄 Strumenti di gestione Web		
Microsoft Defender Application Guard		
🗄 🔲 MultiPoint Connector		
Piattaforma macchina virtuale		
Piattaforma Windows Hypervisor		
Processo di scrittura documenti XPS Microsoft		~
	-	
OK	Annu	ulla

IIS si puo' gestire tramite l'applicazione Windows "Gestione Internet Information Services" avviabile dalla finestra cerca digitando IIS.

Sestione Internet Information Services (IIS)	– 🗆 X
Gerating States (States) </th <th>🖾 🖂 🚱 🗸</th>	🖾 🖂 🚱 🗸
<u>File Visualizza ?</u>	
Connessioni	Azioni
Home page of DESKTOP-LK5 (Q96	Gestisci server
> 🖣 DESKTOP-LK51Q96 (DESKTOP Filtro: 🔹 🍸 Vai 👻 😡 Mostra tutti Raggruppa per:	Z Riavvia
ASP.NET	Avvio Arresto
Chiave Compilazi Globalizzaz Impostazioni Livelli di trust Pagine di	Visualizza pool di applicazioni Pagine e Visualizza siti
computer .NET .NET applicazione .NET errore .NET	controlli Modifica versione di .NET Framework
Posta SMTP Provider Recole di Stato Stringhe di	• Ottieni nuovi componenti della piattaforma Web
autorizzazi sessione connessione	?
Autenticaz Esplorazione Filtro Impostazioni Isolamento Messaggi FTP directory FTP richieste FTP SSL FTP utente FTP FTP	Registrazione FTP
Visualizzazione funzionalità Visualizzazione contenuto	
Pronto	€ <u>1</u> .:

IIS usa il linguaggio lato server e' ASP.NET (i cui file di programma hanno estensione .aspx) basato su C#. Di seguito un frammento di file aspx:

```
<% @ Page Language="C#" %>
<%
foreach (string var in Request.ServerVariables)
{
 Response.Write(var + " " + Request[var] + "<br>");
}
%>
```

IL PROTOCOLLO HTTPS (ssl/tls)



No.	Time	Source	Destination		Protocol	Length	Info
	22 0.068116	192.168.1.52	192,168,1,57		TCP	54	443 → 55174 [FIN, ACK] Seg=1330 Ack=526 Win=130816 Len=0
	23 0.068160	192.168.1.52	192.168.1.57	_	TCP	54	443 → 55172 [ACK] Seg=1331 Ack=526 Win=130816 Len=0
	24 0.072485	192.168.1.57	192.168.1.52		тср	54	55172 → 443 [ACK] Seg=526 Ack=1331 Win=64128 Len=0
	25 0.072485	192.168.1.57	192.168.1.52		TCP	54	55174 → 443 [ACK] Seg=526 Ack=1331 Win=64128 Len=0
1	26 0.073817	192.168.1.57	192.168.1.52		TCP	54	55176 → 443 [ACK] Seg=1 Ack=1 Win=64256 Len=0
	27 0.073817	192.168.1.57	192.168.1.52	1	TLSv1.2	571	Client Hello
	28 0.084807	192.168.1.52	192.168.1.57	2	TLSv1.2	1383	Server Hello, Certificate, Server Key Exchange, Server Hello Done
	29 0.097178	192.168.1.57	192.168.1.52		TCP	54	55176 → 443 [ACK] Seq=518 Ack=1330 Win=64128 Len=0
	30 0.097178	192.168.1.57	192.168.1.52	3	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
	31 0.097178	192.168.1.57	192.168.1.52		TLSv1.2	777	Application Data
	32 0.097379	192.168.1.52	192.168.1.57		TCP	54	443 → 55176 [ACK] Seq=1330 Ack=1367 Win=129792 Len=0
	33 0.098747	192.168.1.52	192.168.1.57	4	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
	34 0.107779	192.168.1.52	192.168.1.57		TLSv1.2	527	Application Data
	35 0.114912	192.168.1.57	192.168.1.52		TCP	54	55176 → 443 [ACK] Seq=1367 Ack=2061 Win=64128 Len=0
	36 0.278686	192.168.1.57	192.168.1.52		TLSv1.2	676	Application Data
	37 0.281028	192.168.1.52	192.168.1.57		TLSv1.2	1514	Application Data
_	38 0 281028	102 168 1 52	192 168 1 57		TCP	1514	113 - 55176 [ACV] San-3531 Ack-1980 Win-131338 Lan-1160 [TCD comment of a reassamb
> F	rame 27: 571 byt	es on wire (4568 b	oits), 571 bytes cap	tured (450	68 bits) on i	nterface	\Device\NPF_{2634871C-619E-44FD-810F-F3EE7243C6C9}, id 0
> E	thernet II, Src:	LiteonTe_0b:c9:31	(20:68:9d:0b:c9:31), Dst: Li	teonTe_8f:e2	:59 (3c:a	0:67:8f:e2:59)
<u>э</u> т	sternet Protocol	Version 4 Sec. 1	92 168 1 57 Det 1	92 168 1 4	2		

Transmission Control Protocol, Src Port: 55176, Dst Port: 443, Seq: 1, Ack: 1, Len: 517

Source Port: 55176

Destination Port: 443 [Stream index: 2]

1 In packet 160, the client sends a Client Hello message that starts the negotiation

2 The server answers with a Server Hello message E The server sends a certilicate to the client.

3 The client takes the certiicate and generates a premaster key.

4 The server creates the master key, and the conversation begins

Nel passaggio 1, il pacchetto 27 è un messaggio Client Hello che è il primo pacchetto nell'handshake TLS . Alcuni dei parametri sono mostrati nello screenshot seguente:

Wireshark - Pacchetto 27 - nod.pcap	-		
Transport Layer Security			_
Y TLSv1.2 Record Laver: Handshake Protocol: Client Hello			
Content Type: Handshake (22)			
Version: TLS 1.0 (0x0301)			
Length: 512			
✓ Handshake Protocol: Client Hello 2			
Handshake Type: Client Hello (1)			
Length: 508			
Version: TLS 1.2 (0x0303) 3			
✓ Random: 1a907cd567463b3954f09dce23419a4aaec8095db3299208167f0c948fc19132			
GMT Unix Time: Feb 15, 1984 08:05:57.000000000 ora solare Europa occidentale 4			
Random Bytes: 67463b3954f09dce23419a4aaec8095db3299208167f0c948fc19132 5			
Session ID Length: 32			
Session ID: 3e347d49a7cc265a443879737fbfcb6a694483e659b81bd60c5c83adad291000			
Cipher Suites Length: 32			
✓ Cipher Suites (16 suites)			
Cipher Suite: Reserved (GREASE) (Øxdada)			
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)			
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)			
Cipher Suite: TLS_AES_256_6CM_SHA384 (0x1302)			
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)			
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)			
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)			
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)			
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)			
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)			
			>
000 3c a0 67 8f e2 59 20 68 9d 0b c9 31 08 00 45 00 < <rbr></rbr> ⋅g··Y h ···1··E·			
20000 2C 90 01 91 65 23 20 00 30 00 C3 21 09 00 42 00 C, B. , U T. E.	Chiudi	1	Aiu

1 mostra che il contenuto del pacchetto è un handshake (ssl.record.content_type == 22).

2 mostra che il pacchetto è un messaggio Client Hello inviato dal client al server web. Questo messaggio avvia l'handshake.

3 mostra la versione SSL e TLS più alta supportata da il cliente.

4 mostra l'ora del client che verrà utilizzata nella chiave processo di generazione.

5 mostra i dati casuali generati dal client da utilizzare nel processo di generazione delle chiavi.

6 mostra le cifre supportate dal client. Le cifre sono elencati in ordine di preferenza.

7 mostra i metodi di compressione dei dati supportati dal cliente.

Come mostrato nella figura seguente, il pacchetto 28 è un messaggio Server Hello, che include i seguenti dettagli:

ranok - occitato zo - notopap	-	
rame 28: 1383 bytes on wire (11064 bits), 1383 bytes captured (11064 bits) on interface \Device\NPF {2634871C-619E-44FD-8	10F-F3EE7243C6C9}	, id @
thernet II, Src: LiteonTe 8f:e2:59 (3c:a0:67:8f:e2:59), Dst: LiteonTe 0b:c9:31 (20:68:9d:0b:c9:31)		
nternet Protocol Version 4, Src: 192.168.1.52, Dst: 192.168.1.57		
ransmission Control Protocol, Src Port: 443, Dst Port: 55176, Seq: 1, Ack: 518, Len: 1329		
ransport Layer Security		
TLSv1.2 Record Layer: Handshake Protocol: Server Hello		
Content Type: Handshake (22) 1		
Version: TLS 1.2 (0x0303)		
Length: 76		
✓ Handshake Protocol: Server Hello		
Handshake Type: Server Hello (2) 3		
Length: 72		
Version: TLS 1.2 (0x0303)		
Random: 9d8a0f3a6e9da54fc08f82acdba5811d0a3dcde33365d242331d390a7da0da5f		
GMT Unix Time: Oct 3, 2053 04:19:38.000000000 ora legale Europa occidentale 👍		
Random Bytes: 6e9da54fc08f82acdba5811d0a3dcde33365d242331d390a7da0da5f 5		
Session ID Length: 0		
Cipher Suite: TLS ECDHE RSA WITH AES 256 GCM SHA384 (0xc030)		
Compression Method: null (0) 7		
Extensions Length: 32		
Extension: renegotiation info (len=1)		
> Extension: ec point formats (len=4)		
> Extension: session ticket (leng)		
 Extension: application layer protocol pegotiation (len=11) 		
[JA35_Ful]string: 771.49900.65281-11-35-16]		
[JA35: 2H33:1374dh4ddf06942f92373c0h54h]		
* TISV1.2 Record Laver: Handshake Protocol: Certificate		
Content Type: Handshake (22)		
Version: TIS 1.2 (9x0303)		
Length: 896		
Y Handshake Protocol: Certificate		

1 mostra che il contenuto del pacchetto è un handshake (ssl.record.tipo_contenuto == 22).

2 mostra la versione TLS che verrà utilizzata in questa sessione.

3 mostra che il pacchetto è un messaggio Server Hello inviato da il server al client.

4 mostra l'ora del server utilizzata nel processo di generazione della chiave.

5 mostra i dati casuali generati dal server per utilizzare nel processo di generazione delle chiavi.

6 mostra la suite di crittografia da utilizzare in questa conversazione. Viene scelto dall'elenco delle cifre inviate dal client.

7 mostra il metodo di compressione dei dati che verrà utilizzato la sessione.

Il pacchetto successivo è la risposta del server che emette un certificato:

*nod.pcap

<u>File</u> <u>M</u> odifica	<u>V</u> isualizza	Vaj	<u>C</u> attura <u>A</u>	nalizza	Statistiche	Telefonia	<u>W</u> ireless	Strumenti	Aiut
🧉 🔳 🧟 🖲	📕 🛅 🔀	C	۹ 👄 🔿	2	& ■	€. €.	Q 🎹		

	Dettagli del pacchetto	· ∨ Ridotti o alla	rgati 🗸 🗌 Distingui maiuscole	Stringa	~	stream Tr
No.	Time	Source	Destination	Protocol	Length	Info
1	22 0.068116	192.168.1.52	192.168.1.57	TCP	54	443 → 55174 [FIN, ACK] Seq=1330 Ack=526 Win=130816 Len=0
	23 0.068160	192.168.1.52	192.168.1.57	TCP	54	443 → 55172 [ACK] Seq=1331 Ack=526 Win=130816 Len=0
	24 0.072485	192.168.1.57	192.168.1.52	TCP	54	55172 → 443 [ACK] Seq=526 Ack=1331 Win=64128 Len=0
	25 0.072485	192.168.1.57	192.168.1.52	TCP	54	55174 → 443 [ACK] Seq=526 Ack=1331 Win=64128 Len=0
1	26 0.073817	192.168.1.57	192.168.1.52	TCP	54	55176 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
1	27 0.073817	192.168.1.57	192.168.1.52	TLSv1.2	571	Client Hello
	28 0.084807	192.168.1.52	192.168.1.57	TLSv1.2	1383	Server Hello, Certificate, Server Key Exchange, Server Hello Done
	29 0.097178	192.168.1.57	192.168.1.52	TCP	54	55176 → 443 [ACK] Seq=518 Ack=1330 Win=64128 Len=0
	30 0.097178	192.168.1.57	192.168.1.52	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
	31 0.097178	192.168.1.57	192.168.1.52	TLSv1.2	777	Application Data
	32 0.097379	192.168.1.52	192.168.1.57	TCP	54	443 → 55176 [ACK] Seq=1330 Ack=1367 Win=129792 Len=0
	33 0.098747	192.168.1.52	192.168.1.57	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
	34 0.107779	192.168.1.52	192.168.1.57	TLSv1.2	527	Application Data
	35 0.114912	192.168.1.57	192.168.1.52	тср	54	55176 → 443 [ACK] Seq=1367 Ack=2061 Win=64128 Len=0
	36 0.278686	192.168.1.57	192.168.1.52	TLSv1.2	676	Application Data
	37 0.281028	192.168.1.52	192.168.1.57	TLSv1.2	1514	Application Data
	38 0 281028	102 168 1 52	192 168 1 57	тср	1514	113 - 55176 [ACK] Seg-3521 Ack-1980 Win-131328 Len-1160 [TCD segment of a reascambled D

> Internet Protocol Version 4, Src: 192.168.1.52, Dst: 192.168.1.57 Internet Protocol Version 4, Src: 192.168.1.52, Dst: 192.168.1.57
Transmission Control Protocol, Src Port: 443, Dst Port: 55176, Seq: 1, Ack: 518, Len: 1329
Transport Layer Security
> TLSV1.2 Record Layer: Handshake Protocol: Server Hello
> TLSV1.2 Record Layer: Handshake Protocol: Certificate 1
> TLSV1.2 Record Layer: Handshake Protocol: Server Key Exchange 2
> TLSV1.2 Record Layer: Handshake Protocol: Server Hello Done 3

Dettagli:

Wiresnark - Pacchetto 28 - nod.pcap —		×
✓ TLSv1.2 Record Layer: Handshake Protocol: Certificate		^
Content Type: Handshake (22)		
Version: TLS 1.2 (0x0303)		
Length: 896		
✓ Handshake Protocol: Certificate		
Handshake Type: Certificate (11)		
Length: 892		
Certificates Length: 889		
✓ Certificates (889 bytes)		
Certificate Length: 886		
✓ Certificate: 308203723082025a020900f80ce6973b19a94d300d06092a864886f70d01010b0500307b (pkcs-9-at-emailAddress=my@acme.it,id-at-co	mmonN	1
> signedCertificate		
> algorithmIdentifier (sha256WithRSAEncryption)		
Padding: 0		
encrypted: 60ae0a07012971bc26d8b859e49174dfbbd3ce06a11a73b8dbea6ec515ba0d9c59189f24		
✓ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange		
Content Type: Handshake (22)		
Version: TLS 1.2 (0x0303)		
Length: 333		
➤ Handshake Protocol: Server Key Exchange		
Handshake Type: Server Key Exchange (12)		
Length: 329		
> EC Diffie-Hellman Server Params		
✓ TLSv1.2 Record Laver: Handshake Protocol: Server Hello Done		
Content Type: Handshake (22)		
Version: TLS 1.2 (0x0303)		
Length: 4		
✓ Handshake Protocol: Server Hello Done		
Handshake Type: Server Hello Done (14)		
Length: 0		
	>	
000 20 68 9d 0b c9 31 3c a0 67 8f e2 59 08 00 45 00 h···1<·g·Y··E·		^
		Y
Chiudi	Aiuto	

1 indica che il server invia il comando Certificate, che include il certificato del server. Navigando nel ramo si vedr' l'emittente del certificato, il tempo di validità, algoritmo e altri dati.

2 mostra che il server invia il comando Server Key Exchange (solitamente Difie-Hellman), inclusi i parametri richiesti (chiave pubblica, firma e così via).

3 mostra che il server invia il messaggio Server Hello Done. Questo comando indica che il server ha completato questa fase dell'handshake SSL. Il passo successivo è l'autenticazione del client.

Il pacchetto successivo è la risposta emessa dal server cioe' un certificato.



1 mostra che il client invia il comando Client Key Exchange. Questo comando contiene il segreto premaster creato dal client ed è stato quindi crittografato utilizzando la chiave pubblica del server. Nela crittografia simmetrica le chiavi vengono generate dal client e dal server, in base ai dati scambiati nel file messaggi di saluto client e server.

2 mostra che il client invia la notifica Change Cipher Spec al server. Questo viene fatto per indicare che il cliente utilizzera' le nuove chiavi di sessione per l'hashing e la crittografia.

L'ultimo passaggio è quando il server invia un nuovo ticket di sessione al client come riportato nella figura seguente:

Арр	olica un filtro di visualizz	zazione <ctrl-></ctrl->					
	Dettagli del pacchet	to 🗸 Ridotti o alla	argati 🗸 🗌 Distingui maiusco	le Stringa	~	stream	Tro
No.	Time	Source	Destination	Protocol	Length	Info	
	22 0.068116	192.168.1.52	192.168.1.57	TCP	54	443 → 55174 [FIN, ACK] Seq=1330 Ack=526 Win=130816 Len=0	
	23 0.068160	192.168.1.52	192.168.1.57	TCP	54	443 → 55172 [ACK] Seq=1331 Ack=526 Win=130816 Len=0	
1	24 0.072485	192.168.1.57	192.168.1.52	TCP	54	55172 → 443 [ACK] Seq=526 Ack=1331 Win=64128 Len=0	
	25 0.072485	192.168.1.57	192.168.1.52	TCP	54	55174 → 443 [ACK] Seq=526 Ack=1331 Win=64128 Len=0	
	26 0.073817	192.168.1.57	192.168.1.52	TCP	54	55176 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0	
	27 0.073817	192.168.1.57	192.168.1.52	TLSv1.2	571	Client Hello	
	28 0.084807	192.168.1.52	192.168.1.57	TLSv1.2	1383	Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	29 0.097178	192.168.1.57	192.168.1.52	TCP	54	55176 → 443 [ACK] Seq=518 Ack=1330 Win=64128 Len=0	
	30 0.097178	192.168.1.57	192.168.1.52	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
	31 0.097178	192.168.1.57	192.168.1.52	TLSv1.2	777	Application Data	
	32 0.097379	192.168.1.52	192.168.1.57	TCP	54	443 → 55176 [ACK] Seq=1330 Ack=1367 Win=129792 Len=0	
	33 0.098747	192.168.1.52	192.168.1.57	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message	
	34 0.107779	192.168.1.52	192.168.1.57	TLSv1.2	527	Application Data	
	35 0.114912	192.168.1.57	192.168.1.52	TCP	54	55176 → 443 [ACK] Seq=1367 Ack=2061 Win=64128 Len=0	
	36 0.278686	192.168.1.57	192.168.1.52	TLSv1.2	676	Application Data	
	37 0.281028	192.168.1.52	192.168.1.57	TLSv1.2	1514	Application Data	
	38 0 281028	192 168 1 52	192 168 1 57	тср	151/	113 - 55176 [ACV] Sen-3521 Ack-1980 Win-131328 Len-1160 [TCD segment of a re	accombled DD
> Fr	ame 33: 312 byte	s on wire (2496 b	bits), 312 bytes captured	(2496 bits) on i	nterface	\Device\NPF_{2634871C-619E-44FD-810F-F3EE7243C6C9}, id 0	
> Et	hernet II, Src:	LiteonTe_8f:e2:59	9 (3c:a0:67:8f:e2:59), Dst	: LiteonTe_0b:c9	:31 (20:6	8:9d:0b:c9:31)	
> In	ternet Protocol	Version 4, Src:	192.168.1.52, Dst: 192.168	.1.57			
> Tr	ansmission Contr	ol Protocol, Src	Port: 443, Dst Port: 5517	6, Seq: 1330, Ac	k: 1367,	Len: 258	
V Tr	ansport Layer Se	curity	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				

DECODIFICARE TLS CON WIRESHARK

Impostiamo prima di tutto la variabile d'ambiente SSLKEYLOGFILE su un certo file a nostra scelta, ad esempio:

C:\>set SSLKEYLOGFILE=C:\temp\keylogfile.txt

Scgliamo un URL che risponda al protocollo https come ad esempio:https://calvino.edu.it (possiamo anche utilizzare curl -s https://calvino.edu.it)

Time Sarce Destration Protocol Length Info 9 2.891969 15.160.82.133 192.166.1.52 TCP 60 443 + 52111 [ACK] Seq=1Ack=518 Win=28032 Len=0 12 2.891969 15.160.82.133 192.166.1.52 TLSV.1.2 2975 Server Hello 11 2.891969 15.160.82.133 192.166.1.52 TLSV.1.2 2975 Server Hello 12 2.891969 15.160.82.133 192.166.1.52 TLSV.1.2 375 Certificate, Server Key Keynang, Server Hello Done 13 2.892157 192.168.1.52 15.160.82.133 192.166.1.52 TLSV.1.2 375 Certificate, Server Key Keynang, Change, Chang		zzazione <ctrl-></ctrl->			
9 2.891969 15.160.82.133 192.168.1.52 TCP 60 43 + 52111 [CKL] Seq-1 Ack=518 Win=28032 Len=0 10 2.891969 15.160.82.133 192.168.1.52 TLSV.2 2974 Server Hello 12 2.891969 15.160.82.133 192.168.1.52 TLSV.2 2974 Server Hello 12 2.891969 15.160.82.133 192.168.1.52 TLSV.2 376 Certificate, Server Key Exchange, Server Hello Done 12 2.891969 15.160.82.133 192.168.1.52 TLSV.2 376 Certificate, Server Key Exchange, Server Hello Done 12 2.897884 192.168.1.52 15.160.82.133 TCP 54 Server Key Exchange, Change Cipher Spec, Encrypted Handshake Message 15 2.906103 15.160.82.133 192.168.1.52 TLSV.2 97 Change Cipher Spec, Encrypted Handshake Message 15 2.906103 15.160.82.133 192.168.1.52 TLSV.2 151 fd0.82.42 151 fd0.82 16 2.906639 192.168.1.52 TLSV.2 151 fd0.82 152 151 fd0.82 152 16 2.906639 192.168.1.52 TCP 60 443 + 52111 fA43 [ACK] Seq-462 Ack-702 Win=28032 Len=0 162 13 .07572 15.160.82.133 192.168.1.52 TCP 64 443 + 52111 fA43 [ACK] Seq-462 Ack-702 Win=28032 Len=0	Time	Source	Destination	Protocol	Length Info
10 2.891969 15.166.82.133 192.168.1.52 TCV 2974 Server Hello 12 2.891969 15.166.82.133 192.168.1.52 TCV 1230 443 + 52111 [FSH, ACK] Seq=2921 Ack=518 Min=28032 Len=1176 [TCP segment of a 12 2.891969 15.160.82.133 192.168.1.52 TLSV1.2 376 Certificate, Server Key Exchange, GargeSia Ack=518 Min=28032 Len=1176 [TCP segment of a 13 2.892157 192.168.1.52 15.160.82.133 TCP 54 S2111 + 443 [ACK] Seq=538 Ack=4419 Min=13128 Len=0 14 2.897894 192.168.1.52 TLSV1.2 376 Certificate, Server Key Exchange, Change Cipher Spec, Encrypted Handshake Message 15 2.908103 15.160.82.133 192.168.1.52 TLSV1.2 97 Change Cipher Spec, Encrypted Handshake Message 15 2.908103 15.160.82.133 192.168.1.52 TCP 60 443 + 52111 [ACK] Seq=4462 Ack=702 Win=28032 Len=14600 [TCP segment of a reas 16 3.073572 15.160.82.133 192.168.1.52 TCP 1654 443 + 52111 [ACK] Seq=4202 Ack=792 Win=28032 Len=14600 [TCP segment of a reas 19 3.073584 192.168.1.52 TCP 1654 443 + 52111 [ACK] Seq=4202 Ack=702 Win=28032 Len=14600 [TCP segment of a reas 19 3.086736 15.160.82.133	9 2.891969	15.160.82.133	192.168.1.52	TCP	60 443 → 52111 [ACK] Seq=1 Ack=518 Win=28032 Len=0
11 2.891669 15.160.82.133 192.168.1.52 TCP 1230 443 + 52111 [PSH, ACK] Seq=2921 Ack=518 Win-28032 Len=1176 [TCP segment of a 12 2.891969 15.160.82.133 192.168.1.52 TLSV1.2 376 Certificate, Server Key Exchange, Server Hello Done 13 2.89157 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=518 Ack=419 Win=13128 Len=0 14 2.897694 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=518 Ack=419 Win=13128 Len=0 15 2.960103 15.160.82.133 192.168.1.52 TLSV1.2 39 Change Cipher Spec, Encrypted Handshake Message 16 2.906639 192.168.1.52 15.160.82.133 TLSV1.2 153 Application Data 17 2.957625 15.160.82.133 192.168.1.52 TCP 60 443 + 52111 [ACK] Seq=4462 Ack=702 Win=28032 Len=0 18 3.073572 15.160.82.133 192.168.1.52 TCP 14654 443 + 52111 [ACK] Seq=702 Ack=1962 Win=13128 Len=0 20 3.066736 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=702 Ack=1962 Win=13128 Len=0 21 3.066329 192.168.1.52 TCP 54 52111 + 443 [ACK] Seq=702 Ack=1062 Win=13128 Len=0 23 3.067741 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=	10 2.891969	15.160.82.133	192.168.1.52	TLSv1.2	2974 Server Hello
12 2.891969 15.160.82.133 192.168.1.52 T.Svl.2 376 Certificate, Server Key Exchange, Server Hello Done 13 2.892157 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq-518 Ack+419 Win-13128 Len-0 14 2.89784 192.168.1.52 15.160.82.133 TLSvl.2 19 Clent Key Exchange, Change Cipher Spec, Encrypted Handshake Message 15 2.998183 15.160.82.133 192.168.1.52 TLSvl.2 97 Change Cipher Spec, Encrypted Handshake Message 16 2.996293 192.168.1.52 TLSvl.2 15 LiP detail 156 detail 16 2.996293 192.168.1.52 TCP 60 443 + 52111 [ACK] Seq-4462 Ack-702 Win-28032 Len-14600 [TCP segnent of a reas 19 3.07386 192.168.1.52 TCP 14654 443 + 52111 [ACK] Seq-4462 Ack-702 Win-28032 Len-14600 [TCP segnent of a reas 19 3.07386 192.168.1.52 TCP 14654 443 + 52111 [ACK] Seq-4702 Ack-1962 Win-131328 Len-0 12 3.086726 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq-702 Ack-1962 Win-131328 Len-0 12 3.086726 192.168.1.52 TSV1.2 21954 Application Data 21 3.086729 192.168.1.52 TCP 54 52111 + 443 [ACK] Seq-702 Ack-1962 Win-131328 Len-0 23 3.087241 192.168.1.52 TSV1.2	11 2.891969	15.160.82.133	192.168.1.52	TCP	1230 443 → 52111 [PSH, ACK] Seq=2921 Ack=518 Win=28032 Len=1176 [TCP segment of a
13 2.892157 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=518 Ack=4419 Win=13128 Len=0 14 2.897894 192.168.1.52 15.160.82.133 TLSVL.2 139 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message 16 2.908639 192.168.1.52 15.160.82.133 TLSVL.2 97 Change Cipher Spec, Encrypted Handshake Message 16 2.908639 192.168.1.52 TLSVL.2 97 Change Cipher Spec, Encrypted Handshake Message 17 2.957825 15.160.82.133 192.168.1.52 TCP 60 443 + 52111 (ACK) Seq=4462 Ack=702 Win=28032 Len=4 18 3.073572 15.160.82.133 192.168.1.52 TCP 164 5443 + 52111 (ACK) Seq=4462 Ack=702 Win=28032 Len=4 19 3.073806 192.168.1.52 15.160.82.133 TCP 54 5211 + 443 [ACK] Seq=7462 Ack=702 Win=28032 Len=4 19 3.073806 192.168.1.52 TLSVL2 21954 Application Data 21 3.086736 21 3.086736 15.160.82.133 TCP 54 5211 + 443 [ACK] Seq=702 Ack=40962 Win=131328 Len=0 22 3.087341 192.168.1.52 TLSVL2 21954 Application Data 23 3.087341 23 3.087341 192.168.1.52 TLSVL2 21954 Application Data 24 3.098116 24 3.098116 15.160.	12 2.891969	15.160.82.133	192.168.1.52	TLSv1.2	376 Certificate, Server Key Exchange, Server Hello Done
14 2.87894 192.168.1.52 15.160.82.133 TLSvl.2 139 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message 15 2.908103 192.168.1.52 TLSvl.2 97 Change Cipher Spec, Encrypted Handshake Message 16 2.908039 192.168.1.52 TLSvl.2 97 Change Cipher Spec, Encrypted Handshake Message 17 2.957825 15.160.82.133 192.168.1.52 TCP 60 434 > 52111 [AK] Seq=4462 Ack=702 Win=28032 Len=0 18 3.073727 15.160.82.133 192.168.1.52 TCP 16454 443 > 52111 [AK] Seq=4462 Ack=702 Win=28032 Len=0 19 3.073808 192.168.1.52 TCP 16454 443 > 52111 [AK] Seq=4462 Ack=702 Win=28032 Len=0 19 3.073808 192.168.1.52 TCP 54 52111 + 443 [ACK] Seq=702 Ack=19062 Win=131328 Len=0 20 3.086734 15.160.82.133 192.168.1.52 TCP 54 52111 + 443 [ACK] Seq=702 Ack=19062 Win=131328 Len=0 21 3.086734 192.168.1.52 TS.10 21954 Application Data 13 23 3.087341 192.168.1.52 TCP 7554 443 + 52111 [ACK] Seq=702 Ack=49062 Min=131328 Len=0 23 3.087341 192.168.1.52 TCP 7554 443 + 52111 [ACK] Seq=49062 Ack=49062 Min=131328 Len=0 23 3.087341 192.168.1.52 TCP 7554 443 + 52	13 2.892157	192.168.1.52	15.160.82.133	TCP	54 52111 → 443 [ACK] Seq=518 Ack=4419 Win=131328 Len=0
15 2.908183 15.160.82.133 192.168.1.52 TLSv1.2 97 Change Cipher Spec, EncryPted Handshake Message 16 2.908639 192.168.1.52 15.160.82.133 TLSv1.2 153 Application Data 17 2.95725 15.160.82.133 192.168.1.52 TCP 60 443 + 52111 [ACK] Seq=4462 Ack=702 Win=28032 Len=0 18 3.073572 15.160.82.133 192.168.1.52 TCP 16454 443 + 52111 [ACK] Seq=4462 Ack=702 Win=28032 Len=14600 [TCP segment of a reas 19 3.073680 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=702 Ack=3062 Win=28032 Len=14000 [TCP segment of a reas 20 3.066736 15.160.82.133 192.168.1.52 TCP 54 52111 + 443 [ACK] Seq=702 Ack=3062 Win=131328 Len=0 21 3.066726 15.160.82.133 192.168.1.52 TCP 7354 443 + 52111 [ACK] Seq=702 Ack=3062 Win=131328 Len=0 22 3.067261 15.160.82.133 192.168.1.52 TCP 7354 443 + 52111 [ACK] Seq=702 Ack=3062 Win=131328 Len=0 23 3.087341 192.168.1.52 TCP 7354 443 + 52111 [ACK] Seq=702 Ack=3062 Win=131328 Len=0 24 3.098146 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=702 Ack=3622 Win=131328 Len=0 24 3.098146 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=702 Ack=3622 Win=131328	14 2.897894	192.168.1.52	15.160.82.133	TLSv1.2	139 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
16 2.900633 192.168.1.52 15.160.62.133 TLSv1.2 153 [ApplIcation Data 17 2.957825 15.160.62.133 192.168.1.52 TCP 60 443 + 52111 [ACK] Seq=4462 Ack=702 Win=28032 Len=0 18 3.07357825 15.160.82.133 192.168.1.52 TCP 60 443 + 52111 [ACK] Seq=4462 Ack=702 Win=28032 Len=0 19 3.073808 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=702 Ack=1962 Win=131328 Len=0 20 3.086736 15.160.82.133 192.168.1.52 TLSv1.2 21954 Application Data 21 3.080529 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=4062 Ack=702 Win=28032 Len=7306 [TCP segment of a reas 23 3.087341 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=702 Ack=4062 Win=131328 Len=0 23 3.087341 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=702 Ack=702 Win=28032 Len=7306 [TCP segment of a reas 23 3.087341 192.168.1.52 TS.160.82.133 TCP 54 52111 + 443 [ACK] Seq=702 Ack=702 Win=28032 Len=7306 [TCP segment of a reas 23 3.087341 192.168.1.52 TS.106.82.133 TCP 54 52111 + 443 [ACK] Seq=702 Ack=702 Win=28032 Len=7306 [TCP segment of a reas 23 3.087341 192.168.1.52	15 2.908103	15.160.82.133	192.168.1.52	TLSv1.2	97 Change Cipher Spec, Encrypted Handshake Message
17 2.957825 15.160.82.133 192.168.1.52 TCP 60.43 + 52111 [ACK] Seq-4462 Ack-702 Win-28032 Len=0 18 3.073572 15.160.82.133 192.168.1.52 TCP 14654 443 + 52111 [ACK] Seq-4462 Ack-702 Win-28032 Len=0 19 3.073808 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq-702 Ack-19662 Win-28032 Len=0 20 3.086736 15.160.82.133 192.168.1.52 TS1.2 21954 Application Data, Application Data 21 3.086292 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq-702 Ack-19662 Win-131328 Len=0 22 3.0867261 15.160.82.133 192.168.1.52 TCP 7554 443 + 52111 + 643 [ACK] Seq-702 Ack-48062 Ack-702 Win-28032 Len-7300 [TCP segment of a reas 23 3.087241 192.168.1.52 TCP 7554 443 + 52111 + 643 [ACK] Seq-702 Ack-48062 Ack-702 Win-28032 Len-7300 [TCP segment of a reas 24 3.09816 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq-702 Ack-48062 Win-131328 Len=0 24 3.09816 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq-702 Ack-48062 Win-131328 Len=0 24 3.09816 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq-702 Ack-48062 Win-131328 Len=0 24 3.09816 15.160.82.133 TCP 54 52111 + 443	16 2.908639	192.168.1.52	15.160.82.133	TLSv1.2	153 Application Data
18 3.073572 15.160.82.133 192.168.1.52 TCP 14654 443 + 52111 ACK Seq=4462 Ack=702 Win=28032 Len=14600 [TCP segment of a reas 19 3.073808 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=702 Ack=3062 Win=31328 Len=0 20 3.080573 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=702 Ack=3062 Win=31328 Len=0 21 3.080529 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=702 Ack=3062 Win=31328 Len=0 22 3.0807261 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq=702 Ack=3062 Win=31328 Len=0 23 3.087341 192.168.1.52 TCP 7354 443 + 52111 [ACK] Seq=702 Ack=3062 Win=31328 Len=0 24 3.008116 15.160.82.133 TCP 54 5211 + 443 [ACK] Seq=702 Ack=3062 Win=31328 Len=0 24 3.008116 15.160.82.133 TCP 54 5211 + 443 [ACK] Seq=702 Ack=3062 Win=31328 Len=0 24 3.008116 15.160.82.133 TCP 54 5211 + 443 [ACK] Seq=702 Ack=3062 Win=31328 Len=0 24 3.008116 15.160.82.133 TCP 54 5211 + 443 [ACK] Seq=702 Ack=3062 Win=31328 Len=0 24 3.008116 15.160.82.133 TCP 54 5211 + 443 [ACK] Seq=702 Ack=3062 Win=31328 Len=0 25 contro 15.160.82.133 TCP 54 5211 +	17 2.957825	15.160.82.133	192.168.1.52	TCP	60 443 → 52111 [ACK] Seg=4462 Ack=702 Win=28032 Len=0
19 3.073808 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq-782 Ack=4962 Win=131328 Len=0 20 3.086736 15.160.82.133 192.166.1.52 TLSV.2 21954 Application Data, Application Data 21 3.0866736 15.160.82.133 192.166.1.52 TLSV.2 21954 Application Data, Application Data 23 3.087281 15.160.82.133 192.168.1.52 TCP 54 52111 + 443 [ACK] Seq-702 Ack=40962 Win=131328 Len=0 23 3.087281 15.160.82.133 192.168.1.52 TCP 7554 443 + 52111 = A43 [ACK] Seq-702 Ack=40962 Win=2032 Len=7300 [TCP segment of a reast 23 3.087241 192.166.1.52 TCP 7554 443 + 52111 = A43 [ACK] Seq-702 Ack=4062 Win=131328 Len=0 23 3.087241 192.168.1.52 TCP 7554 443 + 52111 = A43 [ACK] Seq-702 Ack=4062 Ack=702 Win=2032 Len=7300 [TCP segment of a reast 24 3.098116 15.160.82.133 192.168.1.52 TLSV.2 21954 Application Data, Application Data ame 16: 153 Dytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface \Device\UPF_{2634871C-619E-44FD-810F-F3EE7243C6C9}, id 0 6 hernet II, Src: Liteonfe_8frie2:09 (Sci:0F:0F:20), Dst: senentsu_56:fb:20 (04:71:53:56:fb:20) HCF1753256:fb:20 HCF1753256:fb:20 iternet Protocol Version 4, Src: 192.168.1.52, Dst: 15.160.82.133 mansission Control Pr	18 3.073572	15.160.82.133	192.168.1.52	TCP	14654 443 → 52111 [ACK] Seq=4462 Ack=702 Win=28032 Len=14600 [TCP segment of a reas
20 3.086736 15.160.82.133 192.166.1.52 TLSv1.2 21954 Application Data, Application Data 21 3.086929 192.166.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq-702 Ack=40962 Win=131328 Len=0 23 3.087741 192.166.1.52 TCP 7354 443 + 52111 [ACK] Seq-702 Ack=40962 Win=131328 Len=0 23 3.087741 192.166.1.52 TCP 7354 443 + 52111 [ACK] Seq-702 Ack=4062 Win=131328 Len=0 23 3.087741 192.166.1.52 TCP 54 52111 + 443 [ACK] Seq-702 Ack=4062 Win=131328 Len=0 24 3.087741 192.166.1.52 TLSV1.2 21954 Application Data 24 3.087741 192.166.1.51 192.166.1.52 TLSV1.2 21954 Application Data 24 3.087161 15.160.82.133 TCP 54 52111 + 443 [ACK] Seq-702 Ack=4862 Win=131328 Len=0 24 3.087161 15.160.82.133 TLSV1.2 21954 Application Data Application Data 43 .08016 15.160.82.133 TLSV1.2 21954 Application Data Application Data -ame 16: 153 Systes nametsion Control FASTA Sec.152.0 Sot: 15.160.82.133	19 3.073808	192.168.1.52	15.160.82.133	TCP	54 52111 → 443 [ACK] Seg=702 Ack=19062 Win=131328 Len=0
21 3.086629 192.168.1.52 15.160.82.133 TCP 54.52111 + 443 FAX Seq=702 Ack=40962 Win=131328 Len=0 22 3.087281 15.160.82.133 192.168.1.52 TCP 754 443 +52111 +K1 Seq=40962 Ack=40962 Win=20032 Len=7300 [TCP 535 443 +52111 #K1 Seq=40962 Ack=4062 Win=20032 Len=7300 [TCP sg=40962 Ack=4062 Win=20032 Len=7300 [TCP sg=40962 Ack=4062 Win=20032 Len=7300 [TCP sg=40962 Ack=4062 Win=131328 Len=0 sg=40962 Ack=4062 Win=131328 Len=90 Sg=40962 Ack=4062 Win=131328 Len=90 Sg=40962 Ack=4062 Win=131328 Len=0 Sg=40962 Ack=4062 Win=131328 Len=90 Sg=40962 Ack=4062 Win=131328 Len=90 Sg=40961 Sg=40961 Sg=40961 Sg=40962 Ack=4062 Win=131328 Len=90 Sg=40961 Sg=40962 Ack=4062 Win=131328 Len=90 Sg=40961 Sg=40961 Sg=40961 Sg=40961 Sg=40961 Sg=40962 Ack=4062 <td>20 3.086736</td> <td>15.160.82.133</td> <td>192.168.1.52</td> <td>TLSv1.2</td> <td>21954 Application Data, Application Data</td>	20 3.086736	15.160.82.133	192.168.1.52	TLSv1.2	21954 Application Data, Application Data
22 3.087281 15.160.82.133 192.168.1.52 TCP 7354 443 > 52111 [ACK] 5eq-40962 Ack=702 kin=20832 Len=7300 [TCP segment of a reas 23 3.087281 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] 5eq-702 Ack=8262 kin=13132 Len=70 24 3.098104 15.160.82.133 TCP 7354 443 > 52111 f ACK] 5eq-40962 Ack=8262 kin=13132 Len=70 Ack=8262 kin=13132 Len=70 ame 16: 153 Bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface VieviceWPF_{2634871C-619E-44FD-810F-F3EE7243C6C9}, id 0 Ack=700 Ack=8262 kin=13132 Len=70 hennet II, Src: LiteonTe_8fie2:59 (3c:a067:8fie2:59), Dst: Sernetsu-56:fb:20 (04:71:53:56:fb:20) Version 4, Src: 192.168.1.52, Dst: 15.160.82.133 ansmort Layer Security Jernet Yendool, Src Port: S2111, Dst Port: 443, Seq: 603, Ack: 4462, Len: 99 ansmort Layer Security	21 3.086929	192.168.1.52	15.160.82.133	TCP	54 52111 → 443 [ACK] Seg=702 Ack=40962 Win=131328 Len=0
23 3.087341 192.168.1.52 15.160.82.133 TCP 54 52111 + 443 [ACK] Seg=702 Ack=48262 Win=131328 Len=0 24 3.088116 15.160.82.133 192.168.1.52 TLSv1.2 21954 Application Data, Application Data ame 16: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface Uncvice\NPF_{2634871C-619E-44FD-810F-F3EE724366C9}, id 0 hernet II, Src: LiteonTe_8f:e2:59 (3c:a0:67:8f:e2:59), Dst: SernetSu_56:fb:20 (04:71:53:56:fb:20) ternet Protocol Version 4, Src: 192.168.1.52, Dst: 15.160.82.133 ansmission Control Protocol, Src Port: 52111, Dst Port: 443, Seg: 603, Ack: 4462, Len: 99 ansport Layer Security	22 3,087281	15,160,82,133	192,168,1,52	TCP	7354 443 → 52111 [ACK] Seg=40962 Ack=702 Win=28032 Len=7300 [TCP segment of a reas
24 3.098116 15.160.82.133 192.168.1.52 TLSv1.2 21954 Application Data, Application Data rame 16: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface \Device\WPF_{2634871C-619E-44FD-810F-F3EE7243C6C9}, id 0 thermet TI, Src: Liteorie 5ries20; (3cai67:37:61:259), Dats: sernetSu_56:fb:20 (04:71:53:56:fb:20) nternet Protocol Version 4, Src: 192.168.1.52, Dst: 15.160.82.133 ramsport Layer Security	23 3,087341	192.168.1.52	15,160,82,133	TCP	54 52111 → 443 [ACK] Seg=702 Ack=48262 Win=131328 Len=0
rame 16: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface \Device\WPF_{2634871C-619E-44FD-810F-F3EE7243C6C9}, id 0 thernet II, Src: LiteonTe_8f:e2:59 (3c:a0:67:8f:e2:59), Dst: SernetSu_56:fb:20 (04:71:53:56:fb:20) nternet Protocol Version 4, Src: 192.168.1.52, Dst: 15.160.82.133 ransmission Control Protocol, Src Port: 52111, Dst Port: 443, Seq: 603, Ack: 4462, Len: 99 ransport Layer Security		15 160 00 100	192 168 1 52	TI 5v1.2	21954 Application Data, Application Data
	24 3.098116 rame 16: 153 byt	es on wire (1224 bits), 153 byt	es captured (1224 bits) on int	erface \Device\NPF	-{2634871C-619E-44FD-810F-F3EE7243C6C9}, id 0
	24 3.098116 rame 16: 153 byt thernet II, Src: neternet Protocol ransmission Cont ransport Layer S 0 44 71 53 56 f 0 08 bb 81 84	<pre>is:100.62.133 ies on wire (1224 bits), 153 byt LiteonTe_Bf:e2:59 (3c:a0:67:8f Version 4, Src: 192.168.1.52, rol Protocol, Src Port: 52111, ecurity b 20 3c a0 67 8f e2 59 08 00 4 0 00 80 06 1e 53 c0 a8 01 34 0</pre>	<pre>tes captured (1224 bits) on int :e2:59), Dst: SernetSu_56:fb:2 Dst: 15.166.82.133 Dst Port: 443, Seq: 603, Ack: 5 00qSV. <. g.Y.E. f a0@S4</pre>	erface \Device\NPf 0 (04:71:53:56:fb: 4462, Len: 99	r_{2634871C-619E-44FD-810F-F3EE7243C6C9}, id 0 20)
) 52 85 cb 8f 01 bb 88 9e 26 1f 78 a8 69 23 50 18 R······ & x·i#P·	24 3.098116 rame 16: 153 byt thernet II, Srcz ransmission Cont ransport Layer 5 0 004 71 53 56 f 0 00 8b 81 8 4 52 85 cb 8f 0	<pre>Is:100.02.133 Is:00.02.133 Is:00.02.13 Is:00.02</pre>	Sec aptured (1224 bits) on int :e2:59), Dst: SernetSu_56:fb:2 Dst: 15.160.82.133 Dst Port: 443, Seq: 603, Ack: 5 00 ·qSV. <·g·Y·E· f a0 ···.0€···5··4· 0 18 R.···.8·x·1#P·	erface \Device\NPf 0 (04:71:53:56:fb: 4462, Len: 99	{2634871C-619E-44FD-810F-F3EE7243C6C9}, id 0 20)
0 52 85 cb 8f 01 bb 88 9e 26 1f 78 a8 69 23 50 18 R & x i#P 0 02 01 c7 f3 00 00 17 03 03 00 5e 23 a6 26 01 6b	24 3.098116 rame 16: 153 byt thernet II, Src: ransmission Cont ransport Layer S 0 04 71 53 56 f 0 00 8b b8 18 4 52 85 cb 8f 0 0 20 17 7 3 0	<pre>is:100.62.133 ies on wire (1224 bits), 153 byt LiteonTe_Bf:e2:59 (3c:a0:67:8f Version 4, Src: 192.168.1.52, rol Protocol, Src Port: 52111, ecurity b 20 3c a0 67 8f e2 59 08 00 4 0 00 80 06 1e 53 c0 a8 01 34 0 0 b 88 9e 26 1f 78 a8 69 23 5 0 00 17 03 08 06 23 a6 26 0 </pre>	11 1124 bits) on int 're2:59), Dst: SernetSu_56:fb:2 Dst: 15.160.82.133 Dst Port: 443, Seq: 603, Ack: 5 00 -qSV- <-g-'Y-E-	erface \Device\NPP 0 (04:71:53:56:fb: 4462, Len: 99	F_{2634871C-619E-44FD-810F-F3EE7243C6C9}, id 0 20)
0 52 85 cb 8f 01 bb 88 9e 26 1f 78 a6 69 23 50 18 R····· & k·v:1#P· 0 20 41 c7 73 00 00 17 03 03 09 05 23 a6 26 61 6b ································	24 3.098116 irame 16: 153 byt ithernet II, Src: internet Protocol iransmission Cont ransport Layer S 0 04 71 53 56 f 0 08 8b 81 84 0 52 85 cb 8f 0 0 20 41 c7 f 30 0 44 65 33 3b f 0 44 65 34 d	Is:100.62.133 es on wire (1224 bits), 153 byt LiteonTe 8f:22.59 (3c:a0:67:47 .Version 4, Src: 192.168.1.52, rol Protocol, Src Port: 52111, ecurity b 20 3c a0 67 8f e2 59 08 00 4 0 00 80 06 1e 53 c0 a8 01 34 0 1 bb 88 9e 26 1f 78 a8 69 23 5 0 00 17 03 03 00 5e 23 a6 26 0 0 da b 62 3 51 54 74 68 3	scaptured (1224 bits) on int :e2:59), Dst: SenetSu_56:fb:2 Dst: 15.160.82.133 Dst Port: 443, Seq: 603, Ack: f a0@S4 0 18 R& x.i#P. 16b	erface \Device\NPF 0 (04:71:53:56:fb: 4462, Len: 99	-{2634871C-619E-44FD-810F-F3EE7243C6C9}, id 0 20)
0 52 85 cb 8f 01 bb 88 9e 26 1f 78 a8 69 23 50 18 R···· & k·k·i#P· 0 20 01 c7 f3 00 00 17 03 03 00 5e 23 a6 26 01 6b ···································	24 3.993116 irame 16: 153 byt ithernet II, Src: internet Protocol ransmission Cont ransport Layer S 0 00 8b b8 18 4 0 22 85 cb 8f 0 0 20 1c 7 f 3 0 44 65 86 dC 0 43 3 b f 0 a4 a6 3 a 3b f 0 a4 a6 5 8 8 dC 0 60 c 1 9 8	<pre>15:100.02.133 is on wire (1224 bits), 153 byt LiteonTe_8f:e2:59 (3c:a0:67:8f Version 4, Src: 192.168.1.52, rol Protocol, Src Port: 52111, ecurity b 20 3c a0 67 8f e2 59 08 00 4 0 00 80 06 1e 53 c0 a8 01 34 0 0 08 00 61 e 53 c0 a8 01 34 0 10 b8 89 e2 51 f78 a8 69 23 5 0 00 17 03 00 5e 23 a6 26 0 0 da b6 03 a9 5f f3 a4 7d 86 3 9 12 c5 f6 a0 41 83 9a 6c 78 0 9 12 c5 f6 a0 41 83 9a 6c 78 0 </pre>	5 00 ·qSV· <· g· Y··E·	erface \Device\NPF 0 (04:71:53:56:fb: 4462, Len: 99	F_{2634871C-619E-44FD-810F-F3EE7243C6C9}, id 0 20)
52 55 cb f1 75 a6 69 26 17 78 69 69 26 17 78 66 57 36 69 17 36 69 27 37 57 36 69 17 57 36 78 57 57 36 78 78 58 58 56 57 57 58 56 56 57 57 57 56 66 66 12 57 68 67 78 60 74 <td< th=""><td>24 3.098116 Frame 16: 153 byt Ethernet II, Src: Internet Protocol Transmission Cont Transport Layer S 00 04 71 53 56 f 00 08 bb 81 84 05 28 5c b 87 0 00 04 07 f 8 00 20 1c 7 f 8 00 a 4 6 3 8 5 b 61 00 a 4 6 5 8 6 d c 00 a 6 c 81 05 8 00 20 51 5 2 c</td><td><pre>Is:100.62.133 is:00.62.133 is:00.62.13 is:00.62.13</pre></td><td>ses captured (1224 bits) on int :e2:59), Dst: SernetSu_56:fb:2 Dst: 15:166.82.133 Dst Port: 443, Seq: 603, Ack: 5 00 .q5V. < g.Y.E.</td> f a0@S4. 0 18 R&x.i#P. 16b<td>erface \Device\NPf 0 (04:71:53:56:fb: 4462, Len: 99</td><td>{2634871C-619E-44FD-810F-F3EE7243C6C9}, id 0 20)</td></td<>	24 3.098116 Frame 16: 153 byt Ethernet II, Src: Internet Protocol Transmission Cont Transport Layer S 00 04 71 53 56 f 00 08 bb 81 84 05 28 5c b 87 0 00 04 07 f 8 00 20 1c 7 f 8 00 a 4 6 3 8 5 b 61 00 a 4 6 5 8 6 d c 00 a 6 c 81 05 8 00 20 51 5 2 c	<pre>Is:100.62.133 is:00.62.133 is:00.62.13 is:00.62.13</pre>	ses captured (1224 bits) on int :e2:59), Dst: SernetSu_56:fb:2 Dst: 15:166.82.133 Dst Port: 443, Seq: 603, Ack: 5 00 .q5V. < g.Y.E.	erface \Device\NPf 0 (04:71:53:56:fb: 4462, Len: 99	{2634871C-619E-44FD-810F-F3EE7243C6C9}, id 0 20)
52 52 55 56 76 76 66 76 <td< th=""><td>24 3.098116 Frame 16: 153 byt Ethernet II, Src: Internet Protocol Transmission Cont Transport Layer 9 0 04 71 53 56 f 0 00 08 b8 18 4 52 85 cb 87 0 0 20 1c 7 53 0 0 44 a6 33 b f 0 44 a6 58 8 dc 0 44 a6 58 8 dc 0 60 ce 81 05 8 0 21 52 51 52 ac 1 a 34 82 8c 9</td><td><pre>Is:100.62.133 Is:00.62.133 Is:00.62.14 Is:00.64.14 I</pre></td><td>ses captured (1224 bits) on int :e2:59), Dst: SenetSu_56:fb:2 Dst: 15.160.82.133 Dst Port: 443, Seq: 603, Ack: 5 00 -q5V. <> g.Y.E. f a0 @</td><td>erface \Device\NPF 0 (04:71:53:56:fb: 4462, Len: 99</td><td>-{2634871C-619E-44FD-810F-F3EE7243C6C9}, 1d 0 20)</td></td<>	24 3.098116 Frame 16: 153 byt Ethernet II, Src: Internet Protocol Transmission Cont Transport Layer 9 0 04 71 53 56 f 0 00 08 b8 18 4 52 85 cb 87 0 0 20 1c 7 53 0 0 44 a6 33 b f 0 44 a6 58 8 dc 0 44 a6 58 8 dc 0 60 ce 81 05 8 0 21 52 51 52 ac 1 a 34 82 8c 9	<pre>Is:100.62.133 Is:00.62.133 Is:00.62.14 Is:00.64.14 I</pre>	ses captured (1224 bits) on int :e2:59), Dst: SenetSu_56:fb:2 Dst: 15.160.82.133 Dst Port: 443, Seq: 603, Ack: 5 00 -q5V. <> g.Y.E. f a0 @	erface \Device\NPF 0 (04:71:53:56:fb: 4462, Len: 99	-{2634871C-619E-44FD-810F-F3EE7243C6C9}, 1d 0 20)

Si nota che il pacchetto 16 contiene i dati criptati ovviamente. Ma ora clicchiamo sempre sul pacchetto 16 e alla voce "Transport Layer Security" del pannello intermedio clicchiamo con il tasto destro del mouse e scegliamo "Preferenze del Protocollo"->"(Pre)-Master-Secret log filename ...":

 *Wi-Fi <u>F</u> ile <u>M</u> odifica <u>V</u> isualiz	za Va <u>i C</u> attura <u>A</u> nalizza <u>S</u> tatistiche	Telefonja <u>W</u> ireless S <u>t</u> rumenti	Aiuto			-	o ×
🧉 🔳 🖉 💿 📘 🛅	🗙 🖸 ९ 🗢 🕾 Ŧ 🛓 📃 🗏	Q Q Q II					
Applica un filtro di visualiz	zazione <ctrl-></ctrl->						+ 🔽
Apri le preferenze di TLS		(Pre)	-Master-Secret log filenam	e: C:/Temp/keylogfile.txt	Sfoglia	OK	Annulla
No. Time	Source	Destination	Protocol	Length Info			
9 2.891969	15.160.82.133	192.168.1.52	TCP	60 443 → 52111 [ACK] Seq=1 Ack=518 Win=28032 Len	=0		
10 2.891969	15.160.82.133	192.168.1.52	TLSv1.2	2974 Server Hello			
11 2.891969	15.160.82.133	192.168.1.52	TCP	1230 443 → 52111 [PSH, ACK] Seq=2921 Ack=518 Win=2	8032 Len=1176 [1	TCP segment o	of a r
12 2.891969	15.160.82.133	192.168.1.52	TLSv1.2	376 Certificate, Server Key Exchange, Server Hell	o Done		
13 2.892157	192.168.1.52	15.160.82.133	TCP	54 52111 → 443 [ACK] Seq=518 Ack=4419 Win=131328	Len=0		
14 2.897894	192.168.1.52	15.160.82.133	TLSv1.2	139 Client Key Exchange, Change Cipher Spec, Encr	ypted Handshake	Message	
15 2.908103	15.160.82.133	192.168.1.52	TLSv1.2	97 Change Cipher Spec, Encrypted Handshake Messa	ge		
16 2.908639	192.168.1.52	15.160.82.133	TLSv1.2	153 Application Data	-		
17 2.957825	15.160.82.133	192.168.1.52	TCP	60 443 → 52111 [ACK] Seg=4462 Ack=702 Win=28032	Len=0		
18 3.073572	15.160.82.133	192.168.1.52	TCP	14654 443 → 52111 [ACK] Seg=4462 Ack=702 Win=28032	Len=14600 [TCP :	segment of a	reass
19 3.073808	192.168.1.52	15,160,82,133	TCP	54 52111 → 443 [ACK] Seg=702 Ack=19062 Win=13132	8 Len=0	0	
20 3.086736	15,160,82,133	192.168.1.52	TLSv1.2	21954 Application Data, Application Data			
21 3,086929	192.168.1.52	15,160,82,133	TCP	54 52111 → 443 [ACK] Sea=702 Ack=40962 Win=13132	8 Len=0		
22 3,087281	15,160,82,133	192,168,1,52	TCP	7354 443 → 52111 [ACK] Seg=40962 Ack=702 Win=28032	Len=7300 [TCP	segment of a	reass
23 3,087341	192.168.1.52	15,160,82,133	TCP	54 52111 → 443 [ACK] Seg=702 Ack=48262 Win=13132	8 Len=0	U	
 > Ethernet 11, SrC: > Internet Protocol > Transmission Contr > Transport Layer Sr > TLSv1.2 Record Content Type Version: TLS 	<pre>Liteonie_srie:/sy (Sciaeiso/isriez) Version 4, Src: 192.168.1.52, Dst: rol Protocol, Src Port: 52111, Dst scurity Layer: Application Data Protocol: :: Application Data (23) : 1 2 (areas)</pre>	53), UST: SenetSu_56:T6:2 15.160.82.133 Port: 443, Seq: 603, Ack: http-over-tls	4462, Len: 99	29)			
0000 04 71 53 56 ft	20 3c a0 67 8f e2 59 08 00 45 00	·aSV· <· e··Y··E·					
0010 00 8b b8 18 40	00 80 06 1e 53 c0 a8 01 34 0f a0	····@··· ·S···4··					
0020 52 85 cb 8f 01	bb 88 9e 26 1f 78 a8 69 23 50 18	R · · · · · · & · x · i#P ·					
0030 02 01 c7 f3 00	00 17 03 03 00 5e 23 a6 26 01 6b	····^#·&·k					
0040 a4 a6 3a 3b fb	da b6 03 a9 5f f3 a4 7d 86 35 09	···;·····_··}·5·					
0050 aa t6 58 6d c9	12 c5 f6 a0 41 83 9a 6c 78 09 d0	··Xm·····A··Ix··					
0000 60 ce 81 05 85	0 DD 41 34 Cb CD e2 96 85 40 13 d0	A4 (0)					
0080 1a 34 82 8c 05	36 94 71 66 27 4d a7 68 fd 70 15	46.a f'M.h.n.					
0090 14 73 84 85 37	64 23 c5 6f	·s··7d#· o					
🔘 🍸 wireshark_Wi-FiE/	NE391.pcapng			Pacchetti: 44 · visualizzati: 44 (100.0%) · scar	tati: 0 (0.0%)		Profilo: Defau

Inseriamo il path del file precedentemente scelto nella casella di testo in alto a destra: "Pre-Master-Secret log filename" e diamo OK

ppilea arr file o ar visaali	zzazione <ctrl-></ctrl->			
Time	Source	Destination	Protocol	Length Info
2 0.000039	LiteonTe_8f:e2:59	SernetSu_56:fb:20	ARP	42 192.168.1.52 is at 3c:a0:67:8f:e2:59
3 2.194517	2001:b07:2e5:bf4a:ed7e:702c:9a07:7f	2001:b07:2e5:bf4a:671:53f	DNS	94 Standard query 0xd6c1 AAAA calvino.edu.it
4 2.199325	2001:b07:2e5:bf4a:671:53ff:fe56:fb20	2001:b07:2e5:bf4a:ed7e:70	DNS	94 Standard query response 0xd6c1 AAAA calvino.edu.it
5 2.203684	192.168.1.52	15.160.82.133	TCP	66 52111 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6 2.221396	15.160.82.133	192.168.1.52	TCP	66 443 → 52111 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM=1 WS=128
7 2.221544	192.168.1.52	15.160.82.133	TCP	54 52111 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
8 2.878530	192.168.1.52	15.160.82.133	TLSv1.2	571 Client Hello
9 2.891969	15.160.82.133	192.168.1.52	TCP	60 443 → 52111 [ACK] Seq=1 Ack=518 Win=28032 Len=0
10 2.891969	15.160.82.133	192.168.1.52	TLSv1.2	2974 Server Hello
11 2.891969	15.160.82.133	192.168.1.52	TCP	1230 443 → 52111 [PSH, ACK] Seq=2921 Ack=518 Win=28032 Len=1176 [TCP segment of a r
12 2.891969	15.160.82.133	192.168.1.52	TLSv1.2	376 Certificate, Server Key Exchange, Server Hello Done
13 2.892157	192.168.1.52	15.160.82.133	TCP	54 52111 → 443 [ACK] Seq=518 Ack=4419 Win=131328 Len=0
14 2.897894	192.168.1.52	15.160.82.133	TLSv1.2	139 Client Key Exchange, Change Cipher Spec, Finished
15 2.908103	15.160.82.133	192.168.1.52	TLSv1.2	97 Change Cipher Spec, Finished
16 2.908639	192.168.1.52	15.160.82.133	HTTP	153 GET / HTTP/1.1
17 2.957825	15.160.82.133	192.168.1.52	TCP	60 443 → 52111 [ACK] Seq=4462 Ack=702 Win=28032 Len=0
	Version 4 Sect 102 168 1 E2 Date 1E	160.82.133	111331301101	
nternet Protocol ransmission Cont ransport Layer S 7 TLSv1.2 Record	roal Protocol, Src Port: 52111, Dst Port: ecurity Layer: Application Data Protocol: http-	: 443, Seq: 603, Ack: 4462, •over-tls	Len: 99	
nternet Protocol ransmission Cont ransport Layer S / TLSv1.2 Record Content Typ	rel Protocol, Src Port: 52111, Dst Port: security Layer: Application Data Protocol: http- e: Application Data (23)	: 443, Seq: 603, Ack: 4462, -over-tls	Len: 99	
nternet Protocol ransmission Cont ransport Layer S r TLSv1.2 Record Content Typ	rol Protocol, Src Port: 52110, Dst Port security I Layer: Application Data Protocol: http- e: Application Data (23)	: 443, Seq: 603, Ack: 4462, -over-tls SV· <· g··Y··E·	Len: 99	
nternet Protocol ransmission Cont ransport Layer S TLSv1.2 Record Content Typ 0 04 71 53 56 f 0 08 bb 81 8 4	Tel Person +, 3(c) 192.100.132, 03(c) 13. tecurity 1 Layer: Application Data Protocol: http- e: Application Data (23) 2 0 3 c a0 67 8f e2 59 08 00 45 00 q 0 60 80 06 1e 52 c0 a8 01 34 0f a0	: 443, Seq: 603, Ack: 4462, -over-tls 	Len: 99	
ansmission Cont ansport Layer S TLSv1.2 Record Content Typ 0 44 71 53 56 f 00 8b b8 18 4 52 85 cb 8f 0	Tel Person *, 3(c) 192.100.132, 95(1) Feel Protocol, Src Port: 52111, Dit Port iscurity I Layer: Application Data Protocol: http- e: Application Data (23) 20 2 c a0 67 8 f e2 59 08 00 45 00 - q 0 08 08 06 1e 53 c 08 8 01 34 0 f a0 1 bb 28 9e 26 1f 78 a8 69 23 50 18 R	: 443, Seq: 603, Ack: 4462, -over-tls ISV. <- g - Y - E - @ S 4 	Len: 99	
nternet Protocol ransmission Cont ransport Layer S / TLSv1.2 Record Content Typ 0 04 71 53 56 f 0 00 8b b8 18 4 5 28 5 cb 8f 0 0 20 1 c7 f 3 0	To Participation w, are 192.100.1252, 05:1157. Tech Protocol, Src Port: 52111, Dist Port iscurity I Layer: Application Data Protocol: http- me: Application Data (23) D 20 3c a0 67 8f e2 59 08 00 45 00 - q 0 00 80 06 1e 53 c0 a8 01 34 0f a0 - 1 1b 88 9e 25 1f 78 a8 69 23 59 18 R 0 00 17 03 00 50 52 33 a6 26 01 6t - 5 50 57 56 55 73 a6 26 01 6t - 5 50 57 57 56 57 57 58 57 58 58 58 58 58 58 58 58 58 58 58 58 58	: 443, Seq: 603, Ack: 4462, -over-tls ISV- <- g - YE- 	Len: 99	
nternet Protocol ransmission Cont ransport Layer S / TLSv1.2 Record Content Typ 0 44 71 53 56 f 0 40 8b b8 18 4 52 85 cb 8f 0 0 42 01 7 f 3 0 0 42 6 3 a 3b f 0 40 8 b 8 6 f 0	The Figure 1, Sec. 192.1100.1132, 951.135. Frol Protocol, Sec. Port: S2111, Dit Port. Security I Layer: Application Data Protocol: http- me: Application Data (23) 2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.	: 443, Seq: 603, Ack: 4462, -over-tls SV- <- g-YE- 	Len: 99	
nternet Protocol ansmission Cont TLSV1.2 Record Content Typ 04 71 53 56 f 00 8b b8 18 4 52 85 cb 8f 0 02 01 c7 f3 0 04 46 3a 3b f aa f6 58 6d c5 60 ce 81 05 8	Terp Protocol, Src Port: 52111, Dst Port Fecurity I Layer: Application Data Protocol: http- ie: Application Data (23) b 20 3c a0 67 8f e2 59 08 00 45 00 - 0 00 80 06 1e 53 c0 a8 01 34 0f a0 1 bb 88 9e 25 1f 78 a8 69 23 50 18 R 0 00 17 03 03 00 5e 23 a6 26 01 6b 0 da b 60 3 95 ff 5a 47 26 53 50 9 12 c5 f6 a9 51 88 39 a6 78 09 d0 5 b 41 34 cc bc 2.9 68 54 0f 30	: 443, Seq: 603, Ack: 4462, -over-tls SV: <: g. Y. E. 	Len: 99	
nternet Protocol ransmission Cont ransport Layer S 7 LSV1.2 Record Content Typ 9 04 71 53 56 f 00 8b b8 18 4 52 85 cb 8f 0 02 01 c7 f3 0 0 44 63 a 3b f 0 44 65 88 6d c 0 66 ce 81 05 8 9 92 51 15 2a c	Trol Protocol, Src Port: 52111, Dit Port Security I Layer: Application Data Protocol: http: e: Application Data (23) 0 06 80 06 16 53 c6 80 34 06 40 1 06 80 96 16 53 c6 80 34 06 40 1 06 80 96 16 53 c6 80 34 06 40 1 06 80 96 26 16 73 c8 80 34 06 40 1 06 80 96 26 16 73 c8 80 34 06 40 1 26 56 68 39 56 75 84 74 86 53 69 1 12 c5 76 a9 41 83 96 c7 78 09 00 2 12 c5 76 a9 41 83 96 c7 78 09 00 2 12 c5 76 a9 41 83 96 c7 78 09 00 2 12 c5 76 a9 41 83 96 c7 78 09 00 5 bb 41 34 c5 cb c2 96 85 40 f3 d0 5 bb 41 34 c5 cb c2 96 85 40 f3 d0	: 443, Seq: 603, Ack: 4462, -over-tls SV- <: g-YE- 	Len: 99	
nternet Protocol ransmission Cont ransport Layer S 7 TLSv1.2 Record Content Typ 0 04 71 53 56 f 0 08 8b 81 84 52 85 cb 8f 0 0 20 11 c7 f3 0 0 4 a6 3a 3b f 0 aa f6 58 6d c 66 ce 81 05 8 9 25 1 15 2a c 1a 34 82 8c 9	Teril Protocol, Src Port: 52111, Dit Port: Security I Layer: Application Data Protocol: http: e: Application Data Protocol: http: de 008 06 1e 53 c0 a8 01 34 0f a0 10 b8 89 e2 51 f7 8 a8 69 23 50 18 R 0 00 17 03 03 00 5e 23 a6 26 01 6b 10 b8 89 e3 5f f3 a4 7d 86 35 69 9 12 c5 f6 a9 5f f3 a4 7d 86 35 69 9 12 c5 f6 a9 5f f3 a4 7d 86 35 69 2 a8 he d8 c6 k8 6e 3e 9e c4 b3 a6 2 a8 he d8 c6 k8 6e 3e 9e c4 b3 a6 2 a8 he d8 c6 k8 6e 3e 9e c4 b3 a6 5 a6 pt 61 a6 c2 4d a7 66 fd 70 51 5 a6 pt 61 a6 c2 a4 af 76 6f d7 80 55	: 443, Seq: 603, Ack: 4462, -over-tls SV- <- g-YE- 	Len: 99	

Il pacchetto 16 ora appare in chiaro come evidenziato anche dal dettagio seguente:

📕 Wireshark - Pacchetto 16 - Wi-Fi	×		×
<pre>> Frame 16: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface \Device\NPF_{2634871C-619E-44FD-810F-F3EE7243C > Ethernet II, Src: LiteonTe_8f:e2:59 (3c:a0:67:8f:e2:59), Dst: SernetSu_56:fb:20 (04:71:53:56:fb:20) > Internet Protocol Version 4, Src: 192.168.1.52, Dst: 15.160.82.133 > Transmission Control Protocol, Src Port: 52111, Dst Port: 443, Seq: 603, Ack: 4462, Len: 99</pre>	6C9}, i	id 0	
 TLSv1.2 Record Layer: Application Data Protocol: http-over-tls Content Type: Application Data (23) Version: TLS 1.2 (0x0303) Length: 94 Encrypted Application Data: 23a626016ba4a63a3bfbdab603a95ff3a47d863509aaf6586dc912c5f6a041839a6c7809 			
[Application Data Protocol: http-over-tis] V Hypertext Transfer Protocol			
> GET / HTTP/1.1\r\n			
Host: calvino.edu.it\r\n User-Agent: curl/7.80.0\r\n Accept: */*\r\n			
[HTTP request 1/1]			
[Response in frame: 37]			
0000 04 71 53 56 fb 20 3c a0 67 8f e2 59 08 00 45 00 •oSV• < g ··Y··E·			
0010 00 8b b8 18 40 00 80 06 1e 53 c0 a8 01 34 0f a0			
0020 52 85 cb 87 01 bb 88 9e 26 17 78 a8 69 23 50 18 R······ & x·1#P· 0030 02 11 c7 f3 00 00 17 03 03 00 52 3 a6 26 01 6h ······ ··· ··· ··· ··· ··· ···· ···			
0040 a 6 3a 3b fb da b6 03 a9 5f f3 a4 7d 86 35 09;;			
0050 aa f6 58 6d c9 12 c5 f6 a0 41 83 9a 6c 78 09 d0 ···Xm····· Ā··Ìx··			
0060 60 ce 81 05 85 bb 41 34 c6 cb e2 96 85 40 f3 d0 `			
0070 92 51 15 22 62 64 DE 08 CD 08 65 35 95 64 05 ab 000000000000000000000000000000000			
0090 14 73 84 85 37 64 23 c5 6f ···································			
Frame (153 bytes) Decrypted TLS (78 bytes)			
	hiudi	Ait	Jto