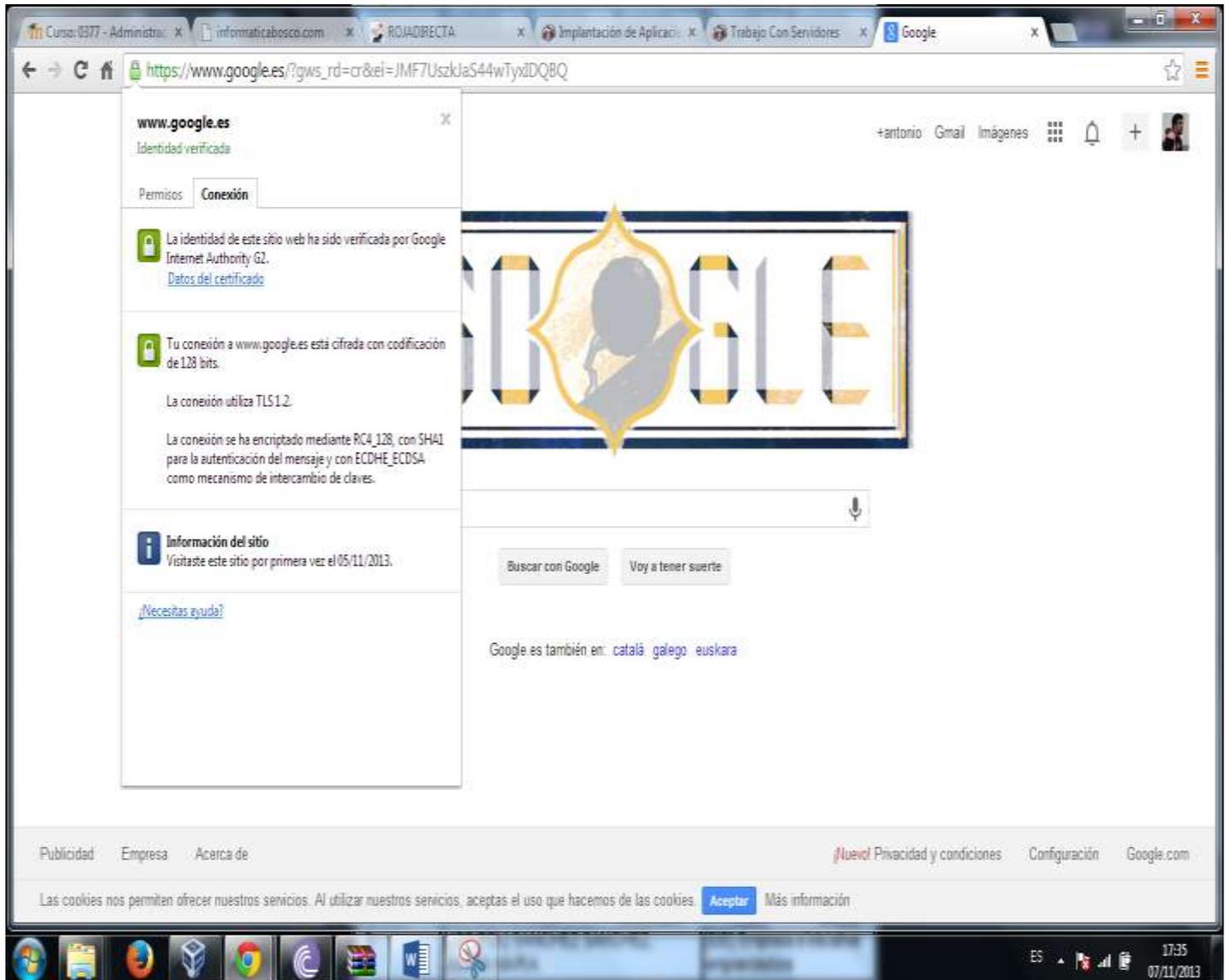


Certificado

Visita una Web que utilice HTTPS y comprueba los siguientes datos: Para quién se emitió el certificado, CA, algoritmo, fecha de caducidad y clave pública. Entregar datos obtenidos y pantallas de capturas

Nos vamos al candado que nos sale a nuestra izquierda del buscador y no sale la información que queremos encontrar



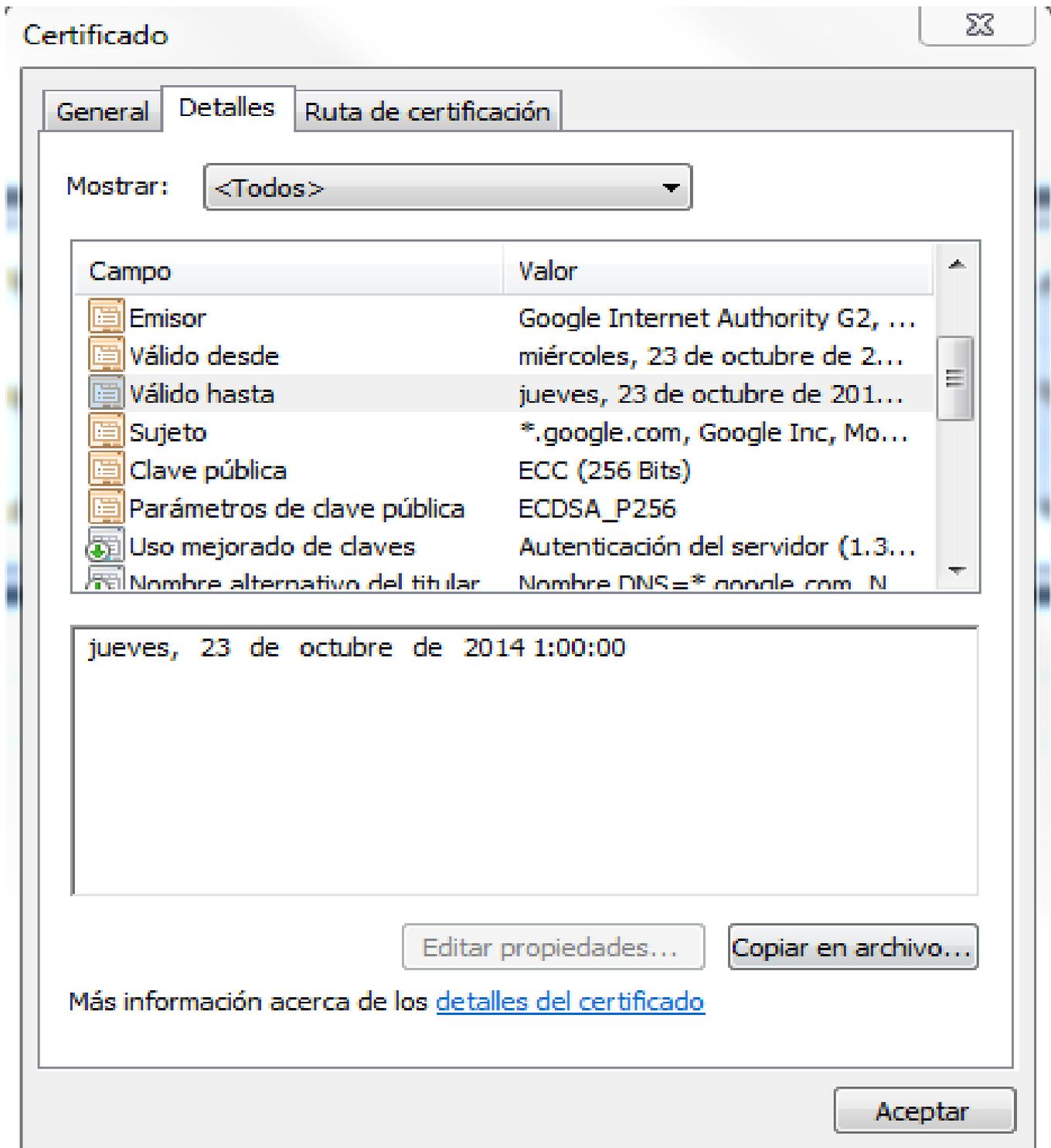
The screenshot shows a web browser window with the Google homepage. A security certificate overlay is visible on the left side of the page. The overlay contains the following information:

- www.google.es** (Identity verified)
- Permisos** / **Conexión**
- La identidad de este sitio web ha sido verificada por Google Internet Authority G2. [Datos del certificado](#)
- Tu conexión a **www.google.es** está cifrada con codificación de 128 bits.
- La conexión utiliza TLS 1.2.
- La conexión se ha encriptado mediante RC4_128, con SHA1 para la autenticación del mensaje y con ECDHE_ECDSA como mecanismo de intercambio de claves.
- Información del sitio**
Visitaste este sitio por primera vez el 05/11/2013.
- [¿Necesitas ayuda?](#)

The background shows the Google homepage with the search bar and navigation links. The system tray at the bottom indicates the date is 07/11/2013 and the time is 17:35.

Certificado

En la pestaña de detalles nos da toda la información como la fecha de emisión ,fecha de caducidad del certificado ,etc...



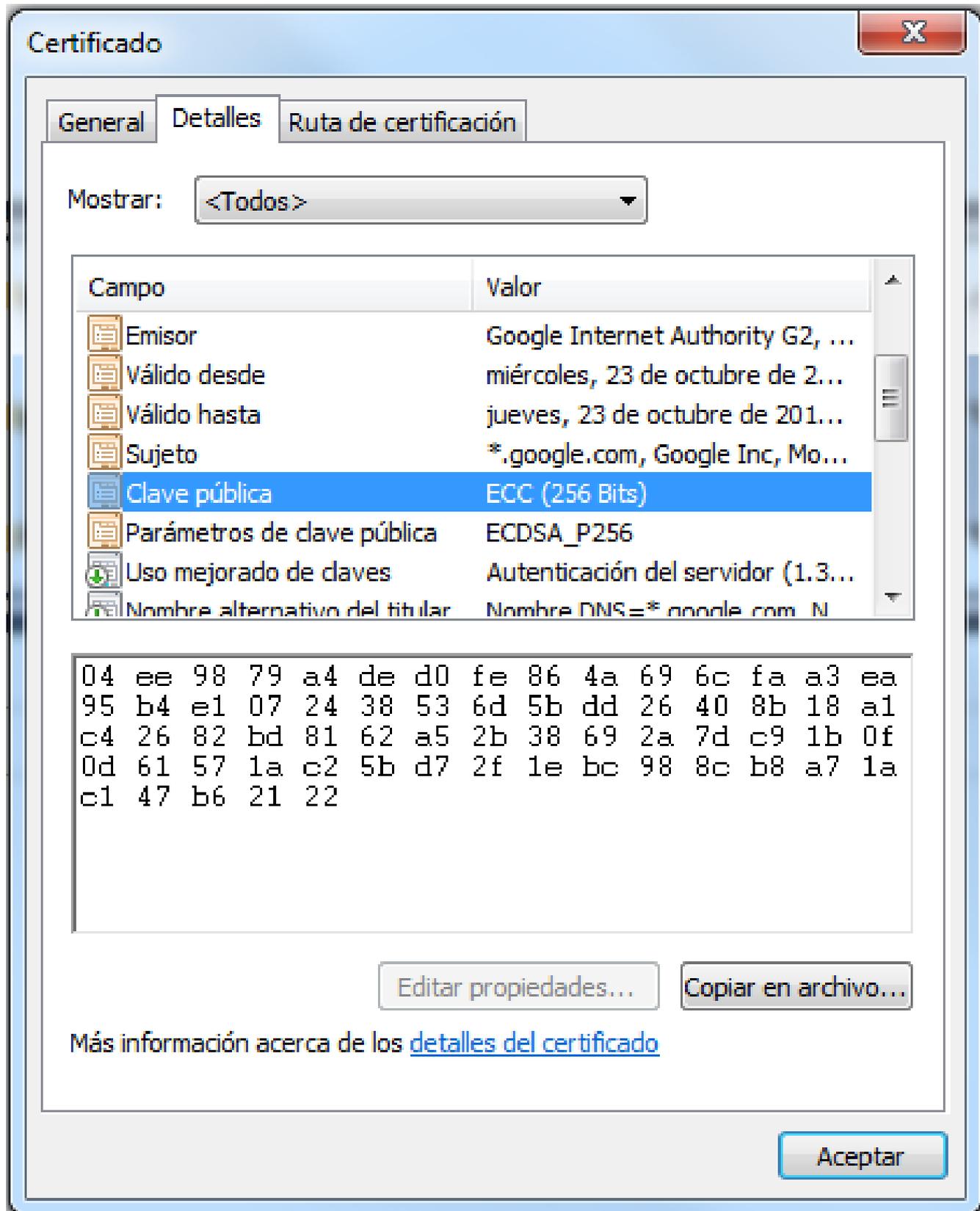
The screenshot shows a Windows dialog box titled "Certificado" with a close button in the top right corner. It has three tabs: "General", "Detalles", and "Ruta de certificación". The "Detalles" tab is selected. Below the tabs is a "Mostrar:" dropdown menu set to "<Todos>". The main content is a table with two columns: "Campo" and "Valor".

Campo	Valor
Emisor	Google Internet Authority G2, ...
Válido desde	miércoles, 23 de octubre de 2...
Válido hasta	jueves, 23 de octubre de 201...
Sujeto	*.google.com, Google Inc, Mo...
Clave pública	ECC (256 Bits)
Parámetros de clave pública	ECDSA_P256
Uso mejorado de claves	Autenticación del servidor (1.3...
Nombre alternativo del titular	Nombre DNS=*.google.com, N...

Below the table is a text box containing the date and time: "jueves, 23 de octubre de 2014 1:00:00". At the bottom of the dialog, there are two buttons: "Editar propiedades..." and "Copiar en archivo...". Below these buttons is a link: "Más información acerca de los [detalles del certificado](#)". At the very bottom right, there is an "Aceptar" button.

Certificado

Como vemos la nos da la clave publica en el certificado.



Certificado

General Detalles Ruta de certificación

Mostrar: <Todos>

Campo	Valor
Emisor	Google Internet Authority G2, ...
Válido desde	miércoles, 23 de octubre de 2...
Válido hasta	jueves, 23 de octubre de 201...
Sujeto	*.google.com, Google Inc, Mo...
Clave pública	ECC (256 Bits)
Parámetros de clave pública	ECDSA_P256
Uso mejorado de claves	Autenticación del servidor (1.3...
Nombre alternativo del titular	Nombre DNS=*.google.com, N

```
04 ee 98 79 a4 de d0 fe 86 4a 69 6c fa a3 ea
95 b4 e1 07 24 38 53 6d 5b dd 26 40 8b 18 a1
c4 26 82 bd 81 62 a5 2b 38 69 2a 7d c9 1b 0f
0d 61 57 1a c2 5b d7 2f 1e bc 98 8c b8 a7 1a
c1 47 b6 21 22
```

Editar propiedades... Copiar en archivo...

Más información acerca de los [detalles del certificado](#)

Aceptar

Certificado

Vemos la información del certificado.

Certificado X

General Detalles Ruta de certificación

 **Información del certificado**

Este certif. está destinado a los siguientes propósitos:

- Asegura la identidad de un equipo remoto
- Prueba su identidad ante un equipo remoto
- 1.3.6.1.4.1.11129.2.5.1

Emitido para: *.google.com

Emitido por: Google Internet Authority G2

Válido desde 23/ 10/ 2013 **hasta** 23/ 10/ 2014

[Declaración del emisor](#)

Obtener más información acerca de [certificados](#)

[Aceptar](#)

Certificado 

General Detalles Ruta de certificación

 **Información del certificado**

Este certif. está destinado a los siguientes propósitos:

- Asegura la identidad de un equipo remoto
- Prueba su identidad ante un equipo remoto
- Protege los mensajes de correo electrónico
- Confirma que el software procede de un editor de software
- Protege el software de alteraciones después de su publicación

Emitido para: GeoTrust Global CA

Emitido por: GeoTrust Global CA

Válido desde 21/ 05/ 2002 **hasta** 21/ 05/ 2022

Obtener más información acerca de [certificados](#)

Certificado

