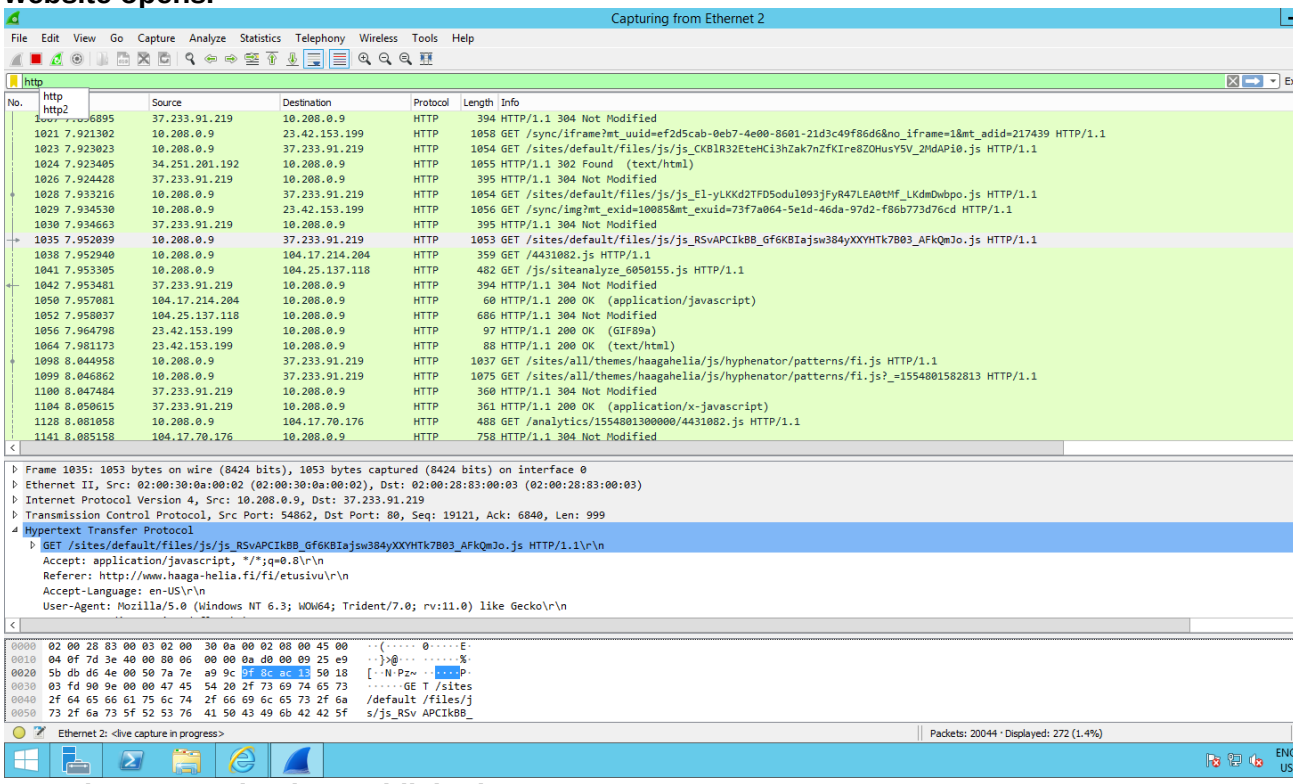
HTTP Monitoring

1. **HTTP is text-based request-response client-server protocol – why can we say so?**
   Ans: When we look first at working of web, the client and the server need to be physically connected, means the computer of the client and the web server. That's the job of the internet, using TCP/IP suite of protocols it establishes the connection using a combination of cable media and wireless media. And doing all this it creates all the necessary work to prepare the environment for the two computers to talk via the HTTP protocol. Once connection is established between client and server, client request as HTTP message and being HTTP connectionless protocol client disconnect from server after its request waiting for response. Server other side process the request, prepare the respond, and again establish connection with client and send back respond in form of HTPP message then again disconnect. HTTP messages used in this communication are plain text. This explains HTTP is a text-based request-response client-server protocol.

2. **How the http connection is usually taking place?**
   Ans: When client makes request to server via HTTP protocol which is based on TCP/IP protocols, server listen to request made by client using its default port 80, process request and respond in the form of HTTP messages. In both cases, connection is disconnected after making request by client and responding by server as HTTP being connectionless protocol. In this way, HTTP connection is taking place.
3. **Access the website www.haaga-helia.fi and monitor the traffic.**

   a) **Write in your browser: http: // www.haaga-helia.fi and capture traffic when the website opens.**



   b) **How the connection is established?**
   Ans: When client made request with server then server responds with HTTP message, in this way connection is established.

   c) **Source and Destination Ports?**
   Source Port: 57464

Destination Port:

d) The client/browser first request?
Client/browser first request GET / HTTP/1.1.\r\n.

e) Response from the server?
When request from source 10.208.0.9 is made to Destination 37.233.91.219 with length 834 and info GET / HTTP / 1.1 then its response is 515 HTTP/1.1 302 Moved Temporarily (Text /hmtl).

f) What HTTP version is used?
HTTP version is 1.1

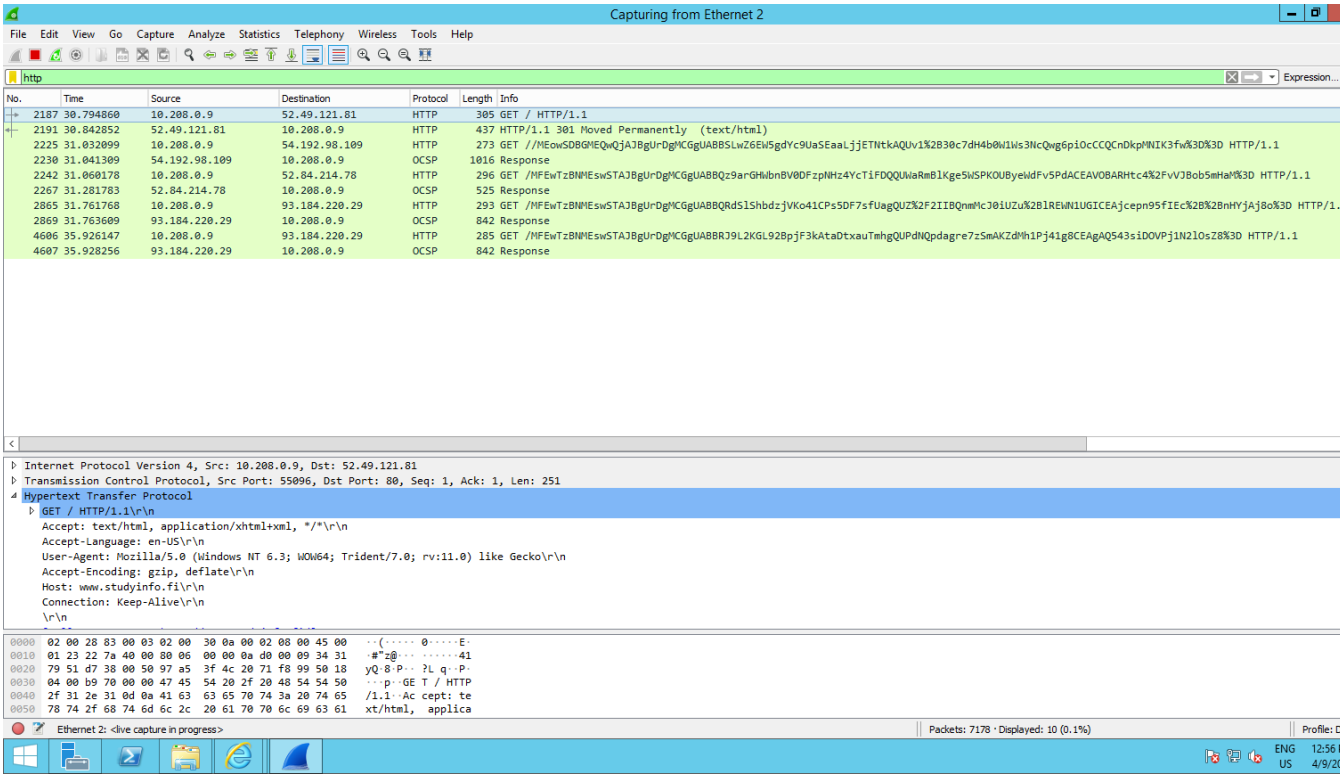
g) What is the web server?
ECS is the web server.

h) Find out, how the data is transferred to the browser?
Ans: When browser sends an HTTP request message to the server for instance asking to send copy of website over internet having TCP/IP protocol, server approves the request and responds the request sending the website's files to browser as a series of small chunks of data packets. When browser receives those packets it assembles the small chunks into a complete website containing text, images, videos and more and displays it to client. In this, the data is transferred to the browser.

4. Access website https://..(your choice).

a) Find out what TLS version is used?
Ans: TLS version used is 1.2v.

b) How Application Data is visible?
Ans:



c) Source and Destination Ports are now?
Ans: Source Port - 53997, Destination Port - HTTPS (443)