Laboratório de análise de Wireshark

Grupo 5

-Bernardo Valente	**87521**
-Francisco Machado	**87530**
-Miguel Aires	**87551**

HTTP Basic Service

---

1. **What is the number of objects of the page?**

   Existem 3 objetos na página.

2. **How many HTTP requests are sent by the client?**

   Foram feitos 7 HTTP Requests.

3. **Is the server able to successfully respond to each one of the requests? How do you know it?**

   O servidor não consegue responder a todos os pedidos.
   Os pedidos de 2 "GET /favicon.ico" e "GET /favicon.ico/" retornaram *"HTTP/1.1 404 Not found(text/html)"* e 2 retornaram *"302 Found"*.

4. **What is the version of HTTP protocol that is used?**

   Versão 1.1.

5. **What type of browser is used to access the site?**

   Firefox (Ubuntu).

6. **What is the URI of the first image requested by the client?**

   http://web.tecnico.ulisboa.pt/~ist13242/basic/cat.jpg

7. **How does the client know that it needs to GET two images to complete the page transfer?**

   Quando o browser recebe o HTML sabe quantas imagens existem na página. No ficheiro HTML existem duas tags de imagens, logo o browser faz dois GET's para ir buscar as imagens.

8. **Does the client wait for the reception of the first image to request the second one?**

Não, os pedidos são feitos em paralelo.

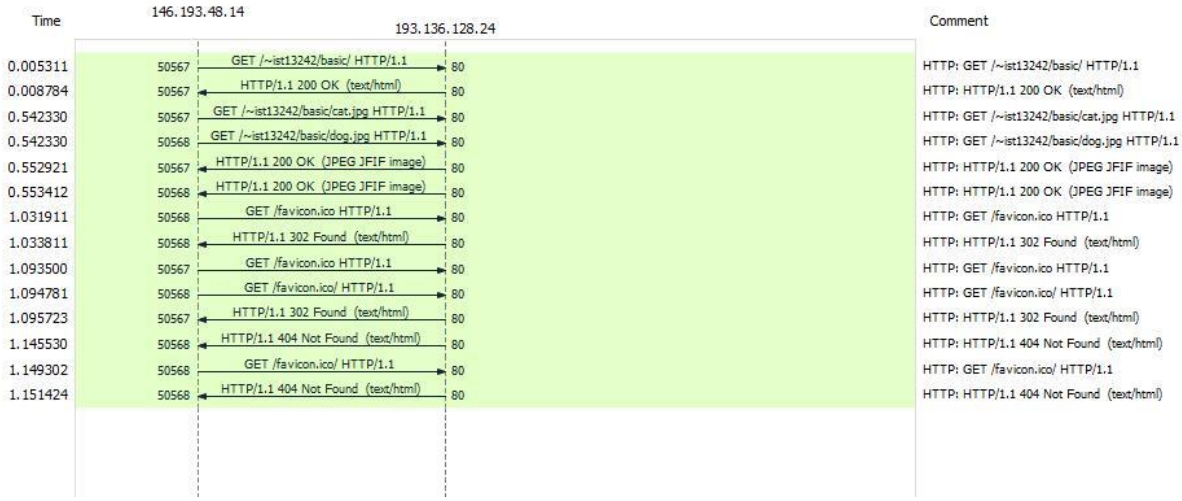
9. **What is the length of the GET message correspondent to the request of the cat.jpg image?**

   O tamanho do GET da request message do ficheiro cat.jpg é 419 bytes.

10. **What is the size of the cat.jpg image?**

    O tamanho da imagem é 117872 bytes. (Content-lenght)

11. **Draw the message diagram that describes the exchange of HTTP messages between the client and the server.**



12. **Remove the HTTP filter. How many TCP connections were established? How many TCP connections were closed?**

    São estabelecidas 2 conexões TCP e 2 conexões TCP foram fechadas.

13. **What are the source and destination IP addresses and ports for each TCP connection?**

    Conexão TCP 1:
    Source: 146.193.48.14. Destination:193.136.128.24
    Source Port: 50567 Destination Port:80
    Conexão TCP 2:
    Source: 146.193.48.14. Destination:193.136.128.24
    Source Port: 50568 Destination Port:80

14. **What is the initial sequence number for the entity that opened the first TCP connection? What is the initial relative sequence number for the entity that opened the first TCP connection?**

Sequence Number: 3501362517
Relative Sequence Number: 0

15. How much time the first TCP connection took to be opened?

Tempo 0.000886s.

HTTP with Authentication

---

16. What is the number of objects of the page?

Existem 3 objetos na página.

17. How many HTTP requests are sent by the client?

6 requests.

18. Why does the server answers with a code "401" when it receives the first request from the client?

Porque o cliente não tem autorização para aceder ao conteúdo da página.

19. What type of HTTP header is included in the "401" response message to inform the client about the expected action?

<head>\n
<title>401 Unauthorized</title>\n
</head>

20. What type of authentication is required?

É necessária uma autenticação com um nome e uma password.

21. What is the message that the user receives in the browser?

"This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required."

22. What new type of HTTP header is included in the second GET message?

É adicionado o seguinte cabeçalho à mensagem GET:
Authorization: Basic aXJjOnNlY3JldGE=\r\n
Credentials: irc:secreta

23. Can you read the username and password from the capture? If so, what are they?

O *username* é irc e a *password* é secreta.
"Credentials: irc:secreta"

24. Is there any difference between the GET messages used to request the cat.jpg image in this example and the GET messages used to request it in the previous example? If yes, what is that difference?

Sim, neste exemplo a mensagem de GET tem um parâmetro adicional com as credenciais de autenticação.

25. Draw the message diagram that describes the exchange of HTTP messages between the client and the server.

HTTP with Forms

26. What is the new method used by the client?

O novo método utilizado pelo cliente é POST.

27. What is the name of the script that was executed by the server?

O nome do script é yourID.php

28. How many items are included in the form?

Há dois itens no form, o *firstname* e *surname*

29. What is the pair (key, value) of the first item?

Key: firstaname
Value: Paulo

30. Is the information of the form transmitted to the server in plain text or is it encrypted?

A informação é transmitida em texto simples porque o wireshark consegue ler o conteúdo dos pacotes (firstname e surname)

31. After receiving the response from the server, what does the user see in the browser?

A resposta do servidor contem uma pagina HTML com o conteúdo:
<html>
<body>
Welcome Paulo
Thank you for submiting the form!
</body>
</html>

32. Is there any dynamic content in the response sent by the server? If so, what is this content?

Sim, existe conteúdo dinâmico porque a resposta contem o texto “Welcome Paulo”, onde “Paulo” é uma variável passada antes pelo o utilizador na mensagem POST.

33. Draw a message diagram that describes the exchange of HTTP messages between the client and the server.