



Lab 2

BÁO CÁO BÀI THỰC HÀNH SỐ 1 PHÂN TÍCH GÓI TIN HTTP VỚI WIRESHARK

Môn học: Nhập môn mạng máy tính

Sinh viên thực hiện	Trần Thanh Hùng (23520580)
Thời gian thực hiện	27/03/2024 – 03/04/2024
Số câu đã hoàn thành	5/5

TRẢ LỜI CÁC CÂU HỎI

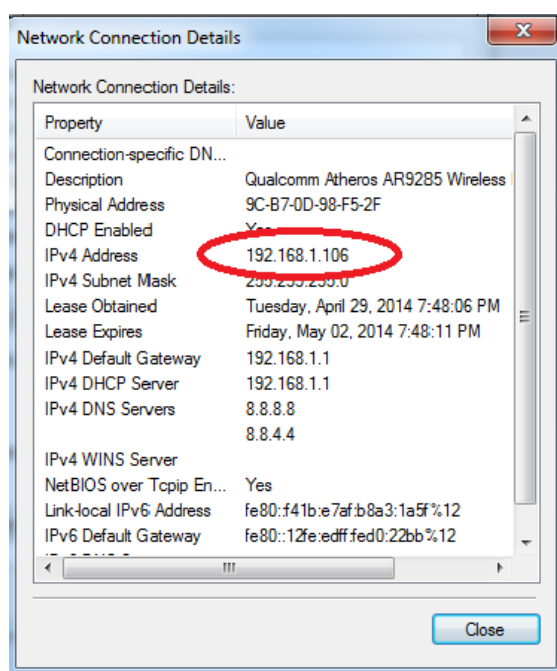
Gợi ý: Trả lời câu hỏi đúng, đầy đủ, cần giải thích lý do tại sao có được đáp án, có các hình ảnh, bằng chứng để chứng minh tính đúng đắn.

Ví dụ:

Câu 1. Địa chỉ IP máy tính của bạn là gì?

Trả lời: 192.168.1.106

Để xem địa chỉ IP của máy tính trên Windows, mở **Control Panel** và chọn **View network status and tasks**. Chọn mạng tương ứng đang sử dụng để kết nối Internet, chọn **Details** trong cửa sổ trạng thái. Xem địa chỉ IP trong Ipv4 Address



1. Trình duyệt đang sử dụng phiên bản HTTP 1.0 hay 1.1? Phiên bản HTTP server đang sử dụng là bao nhiêu?

Trình duyệt đang sử dụng phiên bản HTTP 1.1

Sever đang sử dụng phiên bản HTTP 1.1

2. Địa chỉ IP của máy tính bạn là bao nhiêu? Của web server là bao nhiêu?

IP của máy tính là: 192.168.43.47

IP của web sever là: 192.168.43.23

No.	Time	Source	Destination	Protocol	Length	Info
2641	11.497269	192.168.43.47	192.168.43.23	HTTP	502	GET /23520617.html HTTP/1.1
2645	11.507482	192.168.43.23	192.168.43.47	HTTP	627	HTTP/1.1 200 OK (text/html)

3. Các mã trạng thái (status code) trả về từ server là gì?

Các mã trạng thái (status code) trả về từ sever là: 200

2645	11.507482	192.168.43.23	192.168.43.47	HTTP	627	HTTP/1.1 200 OK (text/html)
------	-----------	---------------	---------------	------	-----	-----------------------------

4. Server đã trả về cho trình duyệt tổng cộng bao nhiêu bytes nội dung?

2641	11.497269	192.168.43.47	192.168.43.23	HTTP	502	GET /23520617.html HTTP/1.1
2645	11.507482	192.168.43.23	192.168.43.47	HTTP	627	HTTP/1.1 200 OK (text/html)
2891	12.468267	192.168.43.47	45.122.249.78	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
2905	12.624956	45.122.249.78	192.168.43.47	HTTP	254	HTTP/1.1 302 Found
3766	18.267239	192.168.43.47	192.168.43.23	HTTP	614	GET /23520617.html HTTP/1.1
3767	18.361174	192.168.43.23	192.168.43.47	HTTP	197	HTTP/1.1 304 Not Modified

Server trả về trình duyệt 627 byte nội dung

5. Xem xét nội dung của HTTP GET đầu tiên. Bạn có thấy dòng “IF-MODIFIEDSINCE” hay không?

Nội dung của HTTP GET đầu tiên không có dòng “IF-MODIFIEDSINCE”

6. Xem xét nội dung phản hồi từ server đối với HTTP GET đầu tiên. Server có trả về nội dung của file HTML hay không? Mã trạng thái đi kèm là gì? Giải thích ý nghĩa.

Từ nội dung phản hồi từ server đối với HTTP Get đầu tiên, server có trả về nội dung file HTML kèm với mã trạng thái 200 OK.

No.	Time	Source	Destination	Protocol	Length	Info
2641	11.497269	192.168.43.47	192.168.43.23	HTTP	502	GET /23520617.html HTTP/1.1
2645	11.507482	192.168.43.23	192.168.43.47	HTTP	627	HTTP/1.1 200 OK (text/html)
2891	12.468267	192.168.43.47	45.122.249.78	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
2905	12.624956	45.122.249.78	192.168.43.47	HTTP	254	HTTP/1.1 302 Found
3766	18.267239	192.168.43.47	192.168.43.23	HTTP	614	GET /23520617.html HTTP/1.1
3767	18.361174	192.168.43.23	192.168.43.47	HTTP	197	HTTP/1.1 304 Not Modified

0040	30 30 20 4f 4b 0d 0a 43	6f 6e 74 65 6e 74 2d 54	00 0K Content-T
0050	79 70 65 3a 20 74 65 78	74 2f 68 74 6d 6c 0d 0a	ype: text/html
0060	4c 61 73 74 2d 4d 6f 64	69 66 69 65 64 3a 20 57	Last-Modified: W
0070	65 64 2c 20 32 37 20 4d	61 72 20 32 30 32 34 20	ed, 27 Mar 2024
0080	30 38 3a 30 32 3a 32 36	20 47 4d 54 0d 0a 41 63	08:02:26 GMT Ac
0090	63 65 70 74 2d 52 61 6e	67 65 73 3a 20 62 79 74	cept-Ranges: byt
00a0	65 73 0d 0a 45 5d 61 67	3a 20 22 30 34 33 37 37	es: "94377
00b0	30 31 62 11 64 30 30 64	61 21 3a 30 22 0d 0a 33	01b1d80d a10" 5
00c0	65 72 76 65 72 3a 20 4d	69 63 72 6f 73 6f 66 74	erver: Microsoft
00d0	2d 49 49 53 2f 31 30 2e	30 0d 0a 44 61 74 65 3a	-IIS/10.0 Date:
00e0	20 57 65 64 2c 20 32 37	20 4d 61 72 20 32 30 32	Wed, 27 Mar 202
00f0	34 20 30 38 3a 30 39 3a	30 39 20 47 4d 54 0d 0a	4 08:09:09 GMT
0100	43 6f 6e 74 65 6e 74 2d	4c 65 6e 67 74 68 3a 20	Content- Length:
0110	33 34 38 0d 0a 0d 0a 3c	21 44 4f 43 54 59 50 45	348<<< !DOCTYPE
0120	20 68 74 6d 6c 3e 0d 0a	3c 68 74 6d 6c 3e 0d 0a	html><<<html><<<
0130	3c 68 65 61 64 3e 0d 0a	3c 74 69 74 6c 65 3e 54	<head><<<title>T
0140	68 e1 bb b1 63 20 68 c3	a0 6e 68 20 6e 68 e1 ba	h<<<c h<<<nh nh<<<
0150	ad 70 20 6d c3 b4 6e 20	6d e1 ba a1 6e 67 20 6d	p m<<<n m<<<ng m
0160	e3 a1 79 20 74 c3 ad 6e	68 20 2d 20 32 3e 2f 74	<<<y t<<<n h<<< 2</t
0170	69 74 6c 65 3e 0d 0a 3c	6d 65 74 61 20 63 68 61	itle><<<meta cha
0180	72 73 65 74 3d 22 75 74	66 2d 38 22 3e 0d 0a 3c	rset="utf-8"><<<
0190	2f 68 65 61 64 3e 0d 0a	3c 62 6f 64 79 3e 0d 0a	/head><<<body><<<
01a0	3c 63 65 6e 74 65 72 3e	3c 69 6d 67 20 0d 0a 73	<center><<<img <<<
01b0	72 63 3d 22 68 74 74 70	3a 2f 2f 70 6f 72 74 61	rc="http://porta
01c0	6c 2e 75 69 74 2e 65 64	75 2e 76 6e 2f 53 74 79	l.uit.ed u.vn/Sty
01d0	6c 65 73 2f 70 72 6f 66	69 2f 69 6d 61 67 65 73	les/prof i/images
01e0	2f 6c 6f 67 6f 31 38 36	78 31 35 30 2e 70 6e 67	/logo186 x150.png
01f0	22 2f 0d 0a 3e 3c 2f 63	65 6e 74 65 72 3e 0d 0a	"<<</c enter><<<
0200	3c 63 65 6e 74 65 72 3e	3c 68 32 3e 4d 53 53 56	<center><<<h2>MSSV
0210	3a 20 32 33 35 32 30 36	31 37 3c 2f 68 32 3e 3c	: 235206 17</h2><
0220	2f 63 65 6e 74 65 72 3e	0d 0a 3c 63 65 6e 74 65	/center><<<cente
0230	72 3e 3c 68 31 3e 20 48	e1 bb 0d 20 76 c3 a0 20	p><<<h1> H<<< v<<<
0240	74 c3 aa 6e 3a 20 4c c3	aa 20 56 c4 a9 6e 68 20	t: n: L<<< V<<<nh
0250	48 75 79 3c 2f 68 31 3e	3c 2f 63 65 6e 74 65 72	Huy<<<h1> /center
0260	3e 0d 0a 3c 2f 62 6f 64	79 3e 0d 0a 3c 2f 68 74	><<<bod y><<</ht
0270	6d 6c 3e		ml>

Mã trạng thái 200 OK được trả về khi máy chủ đáp ứng yêu cầu thành công. Cụ thể, khi máy khách gửi yêu cầu tới máy chủ, nếu máy chủ xử lý yêu cầu thành công và trả về dữ liệu yêu cầu, nó sẽ gửi lại phản hồi với mã trạng thái 200 để cho biết yêu cầu đã được hoàn thành thành công và dữ liệu được trả về đúng như yêu cầu

7. Xem xét nội dung của HTTP GET thứ 2. Bạn có thấy dòng “IF-MODIFIEDSINCE” hay không? Nếu có, giá trị của IF-MODIFIEDSINCE là gì?

Ở nội dung GET thứ 2, có dòng “IF-MODIFIEDSINCE”

No.	Time	Source	Destination	Protocol	Length	Info
2891	12.468267	192.168.43.47	45.122.249.78	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
2905	12.624956	45.122.249.78	192.168.43.47	HTTP	254	HTTP/1.1 302 Found
3766	18.267239	192.168.43.47	192.168.43.23	HTTP	614	GET /23520617.html HTTP/1.1
3767	18.361174	192.168.43.23	192.168.43.47	HTTP	197	HTTP/1.1 304 Not Modified
3768	18.376805	192.168.43.47	45.122.249.78	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
3771	18.486923	45.122.249.78	192.168.43.47	HTTP	254	HTTP/1.1 302 Found
<p>Frame 3766: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bit) on Ethernet II, Src: Intel a6:8a:4c (98:59:7a:a6:8a:4c), Dst: Intel d4:ad:8a:2c (14:35:4b:d4:ad:8a:2c), Internet Protocol Version 4, Src: 192.168.43.47, Dst: 192.168.43.23, Transmission Control Protocol, Src Port: 54853, Dst Port: 8000, Seq: 44, Window: 65535, Len: 614, Win-Bit: 0, Len-Bit: 0, Win-Offset: 0, Len-Offset: 0, Hypertext Transfer Protocol</p> <p>GET /23520617.html HTTP/1.1\r\nHost: 192.168.43.23:8000\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: vi\r\nIf-None-Match: "9437701b1d80d1:0"\r\nIf-Modified-Since: Wed, 27 Mar 2024 08:02:26 GMT\r\n\r\n[Full request URI: http://192.168.43.23:8000/23520617.html]\r\n[HTTP request 2/2]\r\n[Prev request in frame: 2641]\r\n[Response in frame: 3767]</p>						

8. Mã trạng thái HTTP được trả về từ server tương ứng với HTTP GET thứ 2 là gì? Ý nghĩa nó là gì? Server có thật sự gửi về nội dung của file hay không? Giải thích.

- Mã trạng thái HTTP được trả về từ server tương ứng với HTTP GET thứ 2 là 304 Not Modified.

e Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
2891	12.468267	192.168.43.47	45.122.249.78	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
2905	12.624956	45.122.249.78	192.168.43.47	HTTP	254	HTTP/1.1 302 Found
3766	18.267239	192.168.43.47	192.168.43.23	HTTP	614	GET /23520617.html HTTP/1.1
3767	18.361174	192.168.43.23	192.168.43.47	HTTP	197	HTTP/1.1 304 Not Modified
3768	18.376805	192.168.43.47	45.122.249.78	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
3771	18.486923	45.122.249.78	192.168.43.47	HTTP	254	HTTP/1.1 302 Found
<p>Frame 3767: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bit) on Ethernet II, Src: Intel d4:ad:8a:2c (14:35:4b:d4:ad:8a:2c), Dst: Intel a6:8a:4c (98:59:7a:a6:8a:4c), Internet Protocol Version 4, Src: 192.168.43.23, Dst: 192.168.43.47, Transmission Control Protocol, Src Port: 8000, Dst Port: 54853, Seq: 57, Window: 65535, Len: 197, Win-Bit: 0, Len-Bit: 0, Win-Offset: 0, Len-Offset: 0, Hypertext Transfer Protocol</p> <p>HTTP/1.1 304 Not Modified\r\n[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]Response Version: HTTP/1.1Status Code: 304[Status Code Description: Not Modified]Response Phrase: Not ModifiedAccept-Ranges: bytes\r\nETag: "9437701b1d80d1:0"\r\nServer: Microsoft-IIS/10.0\r\nDate: Wed, 27 Mar 2024 08:09:16 GMT\r\n\r\n[HTTP response 2/2][Time since request: 0.093935000 seconds][Prev request in frame: 2641][Prev response in frame: 2645][Request in frame: 3766][Request URI: http://192.168.43.23:8000/23520617.html]</p>						

- 304 Not Modified cho biết rằng tài nguyên được yêu cầu chưa được sửa đổi kể từ lần cuối cùng nó được tải, và không cần phải truyền lại

- Server không gửi nội dung của file HTML mà trình duyệt sẽ lấy nội dung từ cache để hiển thị cho người dùng.

9. Trình duyệt đã gửi bao nhiêu HTTP GET? Đến những địa chỉ IP nào?

Trình duyệt đã gửi 4 HTTP GET đến server (cả sau khi refresh, mỗi lần 2 gói tin HTTP GET) đến những địa chỉ IP: 192.168.43.23 và 45.122.249.78

No.	Time	Source	Destination	Protocol	Length	Info
2641	11.497269	192.168.43.47	192.168.43.23	HTTP	502	GET /23520617.html HTTP/1.1
3766	18.267239	192.168.43.47	192.168.43.23	HTTP	614	GET /23520617.html HTTP/1.1
2891	12.468267	192.168.43.47	45.122.249.78	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
3768	18.376805	192.168.43.47	45.122.249.78	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1

10. Trình duyệt đã gửi bao nhiêu HTTP GET?

Trình duyệt đã gửi 2 file HTTP GET, gói tin thứ 70 (yêu cầu file HTML) và gói tin 114 (yêu cầu favico.ico/ biểu tượng trang web)

No.	Time	Source	Destination	Protocol	Length	Info
62	2.382033	192.168.1.192	128.119.245.12	TCP	66	54935 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
68	2.642192	128.119.245.12	192.168.1.192	TCP	66	80 → 54935 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM=1 WS=128
69	2.642252	192.168.1.192	128.119.245.12	TCP	54	54935 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
70	2.642201	192.168.1.192	128.119.245.12	HTTP	528	GET /index.html HTTP/1.1
100	2.903598	128.119.245.12	192.168.1.192	TCP	60	80 → 54935 [ACK] Seq=1 Ack=475 Win=30336 Len=0
109	2.905229	128.119.245.12	192.168.1.192	TCP	1466	80 → 54935 [ACK] Seq=1 Ack=475 Win=30336 Len=1412 [TCP segment of a reassembled PDU]
110	2.905229	128.119.245.12	192.168.1.192	TCP	1466	80 → 54935 [ACK] Seq=1413 Ack=475 Win=30336 Len=1412 [TCP segment of a reassembled PDU]
111	2.905229	128.119.245.12	192.168.1.192	TCP	1466	80 → 54935 [ACK] Seq=2825 Ack=475 Win=30336 Len=1412 [TCP segment of a reassembled PDU]
112	2.905229	128.119.245.12	192.168.1.192	HTTP	679	HTTP/1.1 200 OK (text/html)
113	2.905294	192.168.1.192	128.119.245.12	TCP	54	54935 → 80 [ACK] Seq=475 Ack=4862 Win=262400 Len=0
114	2.941035	192.168.1.192	128.119.245.12	HTTP	474	GET /favico.ico HTTP/1.1
171	3.203044	128.119.245.12	192.168.1.192	HTTP	538	HTTP/1.1 404 Not Found (text/html)
180	3.255598	192.168.1.192	128.119.245.12	TCP	54	54935 → 80 [ACK] Seq=895 Ack=5346 Win=262144 Len=0

11. Cần bao nhiêu TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights?

Có 3 TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights

111	2.905229	128.119.245.12	192.168.1.192	TCP	1466	80 → 54935 [ACK] Seq=2825 Ack=475 Win=30336 Len=1412 [TCP segment of a reassembled PDU]
110	2.905229	128.119.245.12	192.168.1.192	TCP	1466	80 → 54935 [ACK] Seq=1413 Ack=475 Win=30336 Len=1412 [TCP segment of a reassembled PDU]
109	2.905229	128.119.245.12	192.168.1.192	TCP	1466	80 → 54935 [ACK] Seq=1 Ack=475 Win=30336 Len=1412 [TCP segment of a reassembled PDU]

12. Dòng chữ “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ mấy?

No.	Time	Source	Destination	Protocol	Length	Info
109	2.905229	128.119.245.12	192.168.1.192	TCP	1466	80 → 54935 [ACK] Seq=1 Ack=475 Win=30336 Len=1412 [TCP segment of a reassembled PDU]

Gói tin thứ 109 chứa dòng chữ “THE BILL OF RIGHTS”

13. Mã trạng thái và ý nghĩa nó trong HTTP response tương ứng với HTTP GET đầu tiên là gì?

No.	Time	Source	Destination	Protocol	Length	Info
785	0.654326	192.168.1.192	128.119.245.12	HTTP	544	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
789	0.948191	128.119.245.12	192.168.1.192	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

Mã trạng thái HTTP response tương ứng với HTTP GET đầu tiên là 401 Unauthorized.

Ý nghĩa 401 unauthorized được trả về bởi máy chủ web để cho biết rằng truy cập vào tài nguyên được yêu cầu bị từ chối do không có thông tin xác thực hợp lệ

14. Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu nào mới nào xuất hiện trong HTTP GET?

Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu mới kèm status code 200 OK kèm theo nội dung trang web

813	13.653796	192.168.1.192	128.119.245.12	HTTP	629	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
814	13.992588	128.119.245.12	192.168.1.192	HTTP	543	HTTP/1.1 200 OK (text/html)

▶	Frame 814: 543 bytes on wire (4344 bits), 543 bytes captured (4344 bits) on interface \Device\NPF_{6CE3E112-9429-45CB-8CD6-BE8181BF8B7A}, id 0	0000	04 7c
▶	Ethernet II, Src: HuaweiTechno_20:1f:db (d4:4f:67:20:1f:db), Dst: MicroStarINT_a3:f5:5e (04:7c:16:a3:f5:5e)	0010	02 11
▶	Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.192	0020	01 c0
▶	Transmission Control Protocol, Src Port: 80, Dst Port: 51822, Seq: 718, Ack: 1066, Len: 489	0030	00 f6
▶	Hypertext Transfer Protocol	0040	30 30
▶	HTTP/1.1 200 OK\r\n	0050	2c 20
▶	[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]	0060	3a 32
▶	Response Version: HTTP/1.1	0070	65 72
▶	Status Code: 200	0080	20 28
▶	[Status Code Description: OK]	0090	4c 2f
▶	Response Phrase: OK	00a0	50 2f
▶	Date: Wed, 03 Apr 2024 11:28:51 GMT\r\n	00b0	6c 2f
▶	Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n	00c0	2e 31
▶	Last-Modified: Wed, 03 Apr 2024 05:59:01 GMT\r\n	00d0	66 69
▶	ETag: "84-6152aeb59ac9e"\r\n	00e0	72 20
▶	Accept-Ranges: bytes\r\n	00f0	47 4d
▶	Content-Length: 132\r\n	0100	31 35
▶	[Content length: 132]	0110	63 63
▶	Keep-Alive: timeout=5, max=99\r\n	0120	74 65
▶	Connection: Keep-Alive\r\n	0130	67 74
▶	Content-Type: text/html; charset=UTF-8\r\n	0140	6c 69
▶	\r\n	0150	20 6d
▶	[HTTP response 2/2]	0160	69 6f
▶	[Time since request: 0.338792000 seconds]	0170	0a 43
▶	[Prev request in frame: 785]	0180	65 78
▶	[Prev response in frame: 789]	0190	74 3d
▶	[Request in frame: 813]	01a0	6c 3e
▶	[Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]	01b0	20 70
▶	File Data: 132 bytes	01c0	74 65
▶	Line-based text data: text/html (6 lines)	01d0	73 65
▶	\n	01e0	27 76
▶	<html>\n	01f0	68 65
▶	\n	0200	79 20
▶	This page is password protected! If you're seeing this, you've downloaded the page correctly \n	0210	61 74
▶	Congratulations!\n		
▶	</html>		