فرم گزارش کار آزمایشگاه شبکه

نام و نام خانوادگی	کیان پورآذر	شماره دانشجویی	۴۰۱۳۱۴۰۳	نام و شماره آزمایش	۴- راه اندازی سرویسهای Webو FTP
هدف آزمایش	آشنایی با تنظیمات مقدماتی مربوط به راه اندازی سرویسهای Web و FTP و تحلیل بسته های FTPو HTTP				
ابزارهای مورد نیاز	کامپیوتر با سیستم عامل ترجیحا ویندوز 7 و برنامه Filezila نسخه 1.0.17.3				
شرح آزمایش	در ابتدا تنظیمات مربوط به سرور وب را انجام میدهیم. سپس تنظیمات مربوط به اضافه کردن سایت تست در iis را انجام میدهیم و فایل تست را مینویسیم. سوال 1: با توجه به اینکه اطلاعات را داخل فایل hosts اضافه نکردیم ،وب سرور به صورت گلوبال دنبال هاست میگردد و به صورت لوکال سایت بالا نمیاید. بعد از اضافه کردن اطلاعات و پاک کردن کش، سایت نمایش داده میشود. سوال 2: وایرشارک نمیتواند هیچ بسته ای از سایت ما را شنود کند چون وایرشارک نمیتواند ترافیک مربوط به آدرس های loopback را شنود کند. برای حل این مشکل از Rawcap استفاده میکنیم و بسته ها را با آن شنود میکنیم سپس فایلی که اطلاعات شنود شده در آن قرار دارد را با وایرشارک باز میکنیم و اطلاعات را میخوانیم. سوال 3: طبق عکس پورت مبدا 64743 و پورت مقصد 80 است. برقراری ارتباط با استفاده از پروتکل TCP و به روش handshaking صورت میگیرد. به گونه ای که ابتدا سیستم یک درخواست به سایت میفرستد و سپس از سایت یک پاسخ میگیرد که به معنای برقراری ارتباط است. با توجه به اینکه ما در فایل hosts مشخص کرده ایم که به ازای www.test.com ، آیپی مورد نظر ما چی باشد وب سرور دیگر برای گرفتن ip متناظر سراغ DNS نمیرود و سایت ما نمایش داده میشود.					

سوال 4: مقدار connection برابر است با keep-alive است و نشان دهنده این است که ارتباط بعد از فرستادن درخواست و گرفتن جواب از بین نمیرود و باز هم میشود با این ارتباط درخواست ارسال کرد.

درخواست HTTP، از نوع GET است به معنی اینکه میخواهد دیتا دریافت کند.
مقدار user agent هم در تصویر زیر مشخص است.

مقدار user agent نشان دهنده نوع سیستم عامل و مرورگر است.
سوال 5: طبق تصویر مقدار flag برابر است با 018x0

سوال 6: سایت جدید hostname و پورت متفاوتی با سایت اولی دارد و در request type و زمان ارسال و حجم بسته ها متفاوت هستند.

سوال 7: با توجه به اینکه پورتی تعریف نشده و دو تا domain برای یک ip درنظرگرفته شده است پس هیچکدام از سایت ها نمایش داده نمیشوند.

سوال 8: بله با مشکل مواجه شدیم. دلیل این اتفاق هم این است که چون در certificate مرورگر و سایت اشتراکی وجود ندارد این دو نمیتوانند با هم ارتباط حفاظت شده برقرار کنند. با استفاده از rawcap اطلاعات را شنود میکنیم و با وایرشارک بسته ها را مشاده میکنیم. در ابتدا درخواست اتصال فرستاده میشود و مرورگر یک key برمیگرداند و از انجایی که key ای که توسط مرورگر فرستاده شده با key موجود یکسان نمیباشد اتصال امن برقرار نمیشود.

سوال 9: طبق تصویر گواهی به نام خودم است که توسط خودم ایجاد شده است. مدت زمان آن یکسال است و الگوریتم آن RSA است و کلید عمومی صادرکننده هم در عکس مشخص است.

سوال 10: خیر نمیتوانیم متن ارتباط را بخوانیم چون توسط TLS رمزنگاری شده است.

سوال 11: طبق عکس این دو خیلی متفاوت هستند برای مثال در الگوریتم رمزنگارش شده، کلید رمزنگاری و تاریخ انقضای گواهی متفاوت هستند.

	از دستور LIST برای لیست کردن دایرکتوری ها استفاده میکنیم .Username, password با توجه به اینکه در وضعیت ناشناس هستیم قابل مشاهده نیست پروتکل لایه انتقال FTP است. آدرس پورت مبدا 21 و مقصد 51126 است. سوال 13: تنظیمات عوض میکنیم و دوباره شنود را انجام میدهیم این بار با توجه به اینکه احراز هویت در وضعیت basic قرار دارد میتوانیم رمزعبور را مشاهده کنیم. سوال 14: 2 سطح دسترسی basic و anonymous وجود دارد. حالا سطح دسترسی داده شده برابر است با: Authentication = basic permissions= read authorization= all users سوال 15: خیر نمیتوانیم وارد شویم. سوال 16: این خطا زمانی رخ میدهد که کاربر بخواهد با http یا FTP به جای TLS استفاده کند و سرور دارد کلاینت را ملزم به این میکند تا یک ارتباط TLS ایجاد کند.
نتیجه-گیری	با پروتکل های HTTP و FTP و نحوه شنود با استفاده از Rawcap اشنا شدیم. توانستیم بسته های HTTPوFTP را تحلیل کنیم. همچنین نحوه بالا اوردن یک سایت و نحوه اعمال انواع تنظیمات برای آن و نحوه رمزنگاری برای آن یکی از نتایج مهم این آزمایش است.

اسکرین شات‌ها:

www.kiyantube.com

HTTP Error 401.3 - Unauthorized

You do not have permission to view this directory or page because of the access control list (ACL) configuration or encryption settings for this resource on the Web server.

Most likely causes:

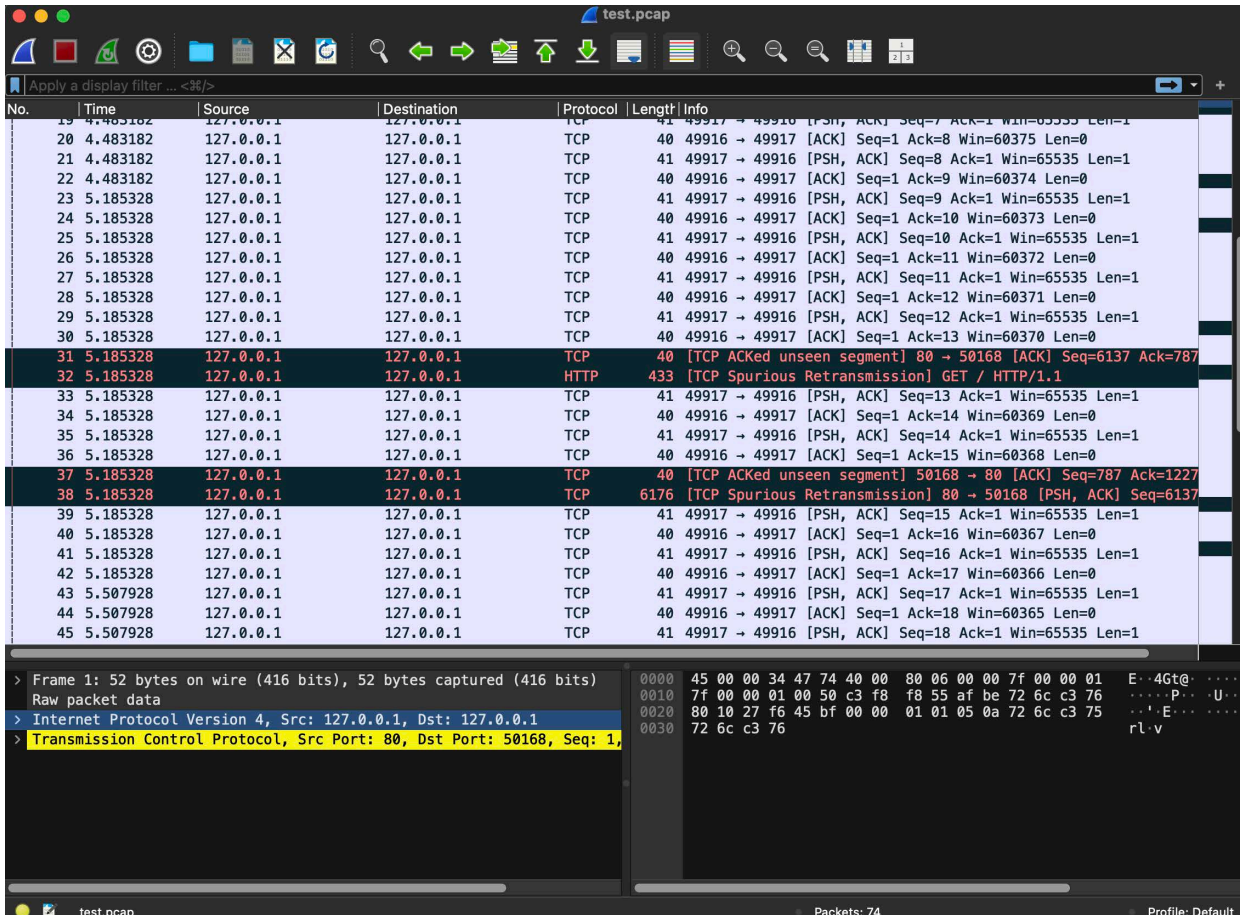
- The user authenticated by the Web server does not have permission to open the file on the file system.
- If the resource is located on a Universal Naming Convention (UNC) share, the authenticated user may not have sufficient share a nd NTFS permissions, or the permissions on the share may not match the permissions on the physical path.
- The file is encrypted.

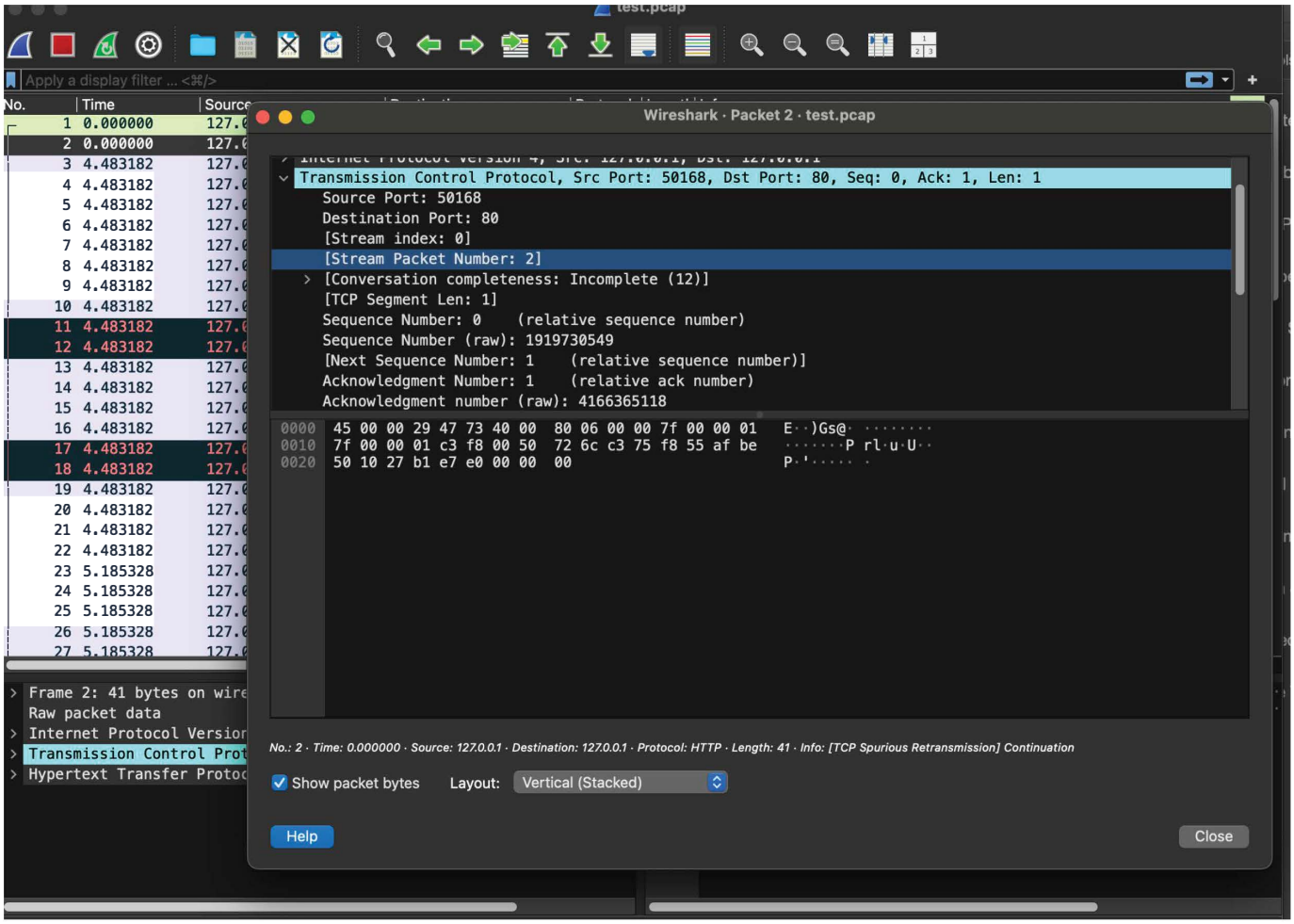
Things you can try:

- Open File Explorer and check the ACLs for the file that is being requested. Make sure that the user accessing the Web site is not b eing explicitly denied access, and that they do have permission to open the file.
- Open File Explorer and check the ACLs for the share and the physical path. Ensure that both ACLs allow the user to access the res ource.
- Open File Explorer and check the encryption properties for the file that is being requested. (This setting is located in the Advance d attribute properties dialog.)
- Create a tracing rule to track failed requests for this HTTP status code. For more information about creating a tracing rule for faile d requests, click **here**.

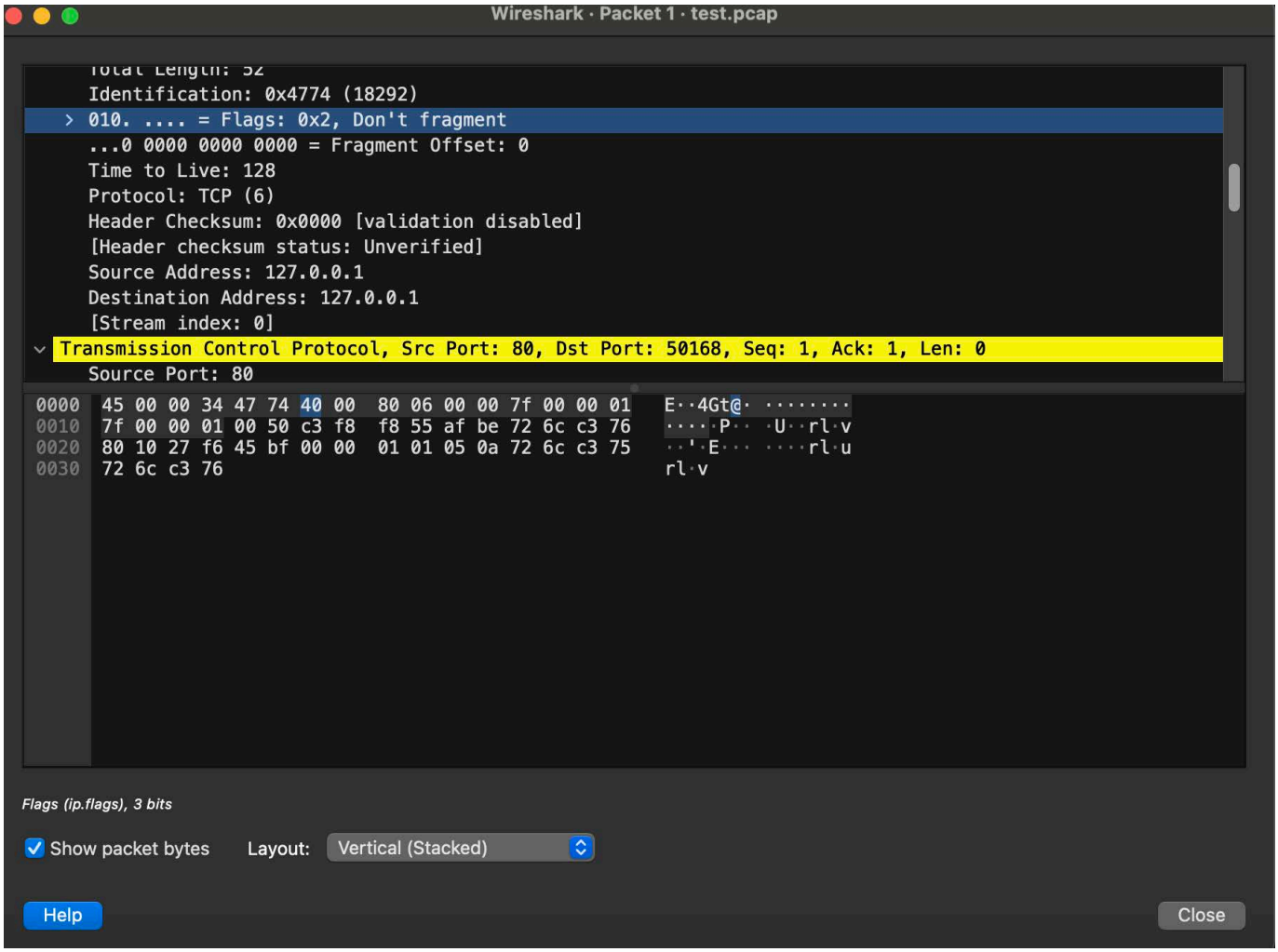
Detailed Error Information:

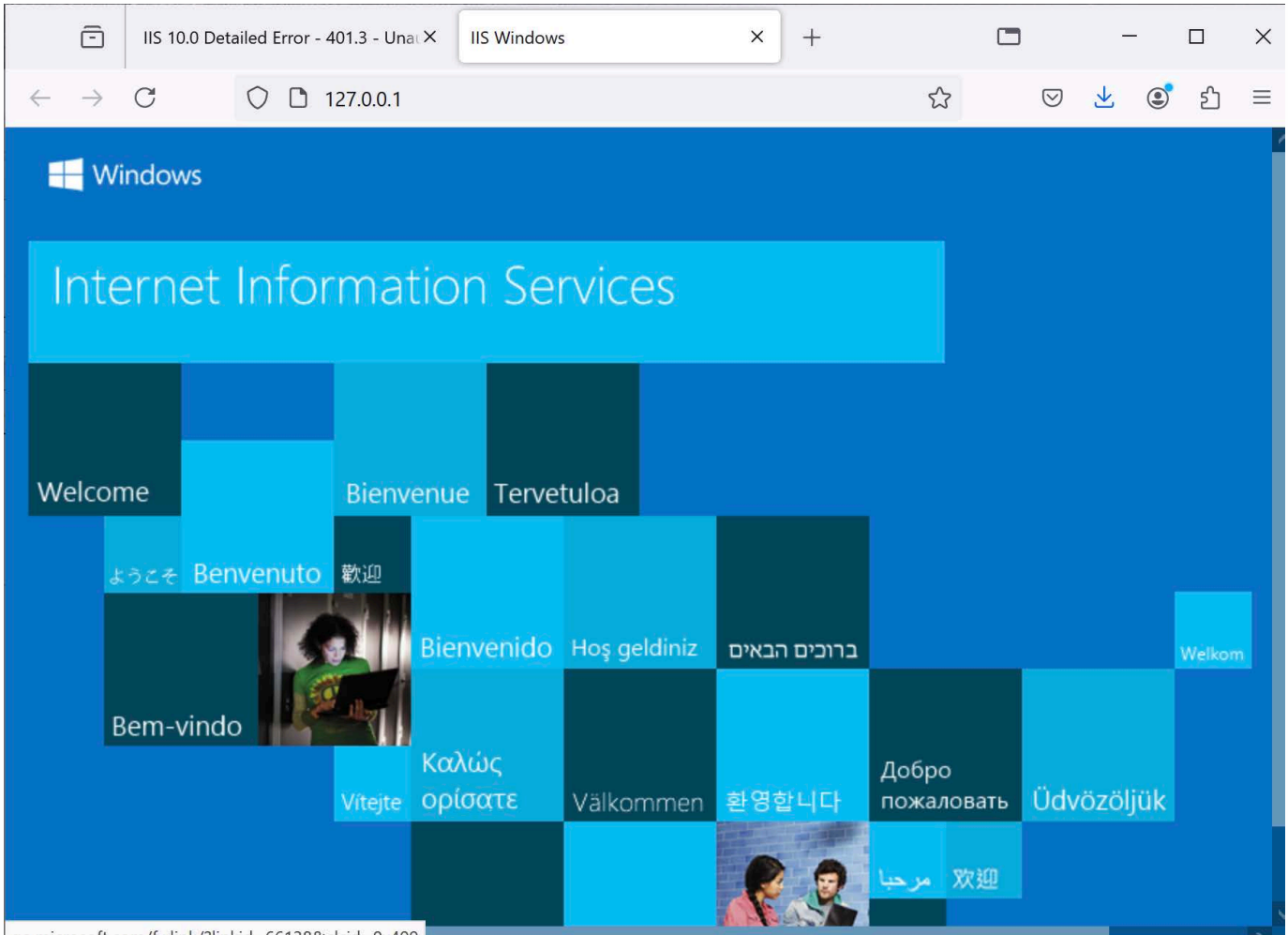
Module	IIS Web Core	**Requested URL**	http://www.kiyantube.com:80/
Notification	AuthenticateRequest	**Physical Path**	C:\Users\Windows\Desktop\New folder
Handler	StaticFile		

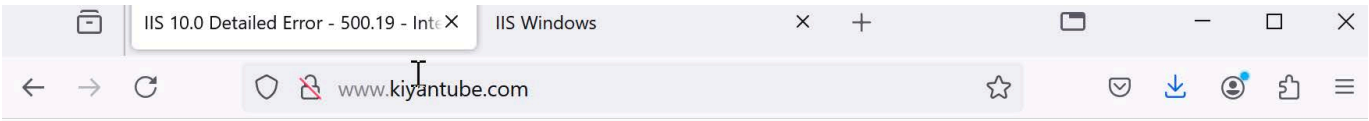



test.pcap
Apply a display filter ... <⌘/>
No. Time Source
1 0.000000 127.0
2 0.000000 127.0
3 4.483182 127.0
4 4.483182 127.0
5 4.483182 127.0
6 4.483182 127.0
7 4.483182 127.0
8 4.483182 127.0
9 4.483182 127.0
10 4.483182 127.0
11 4.483182 127.0
12 4.483182 127.0
13 4.483182 127.0
14 4.483182 127.0
15 4.483182 127.0
16 4.483182 127.0
17 4.483182 127.0
18 4.483182 127.0
19 4.483182 127.0
20 4.483182 127.0
21 4.483182 127.0
22 4.483182 127.0
23 5.185328 127.0
24 5.185328 127.0
25 5.185328 127.0
26 5.185328 127.0
27 5.185328 127.0
Frame 2: 41 bytes on wire
Raw packet data
Internet Protocol Version
Transmission Control Prot
Hypertext Transfer Protoc
Wireshark · Packet 2 · test.pcap
Transmission Control Protocol, Src Port: 50168, Dst Port: 80, Seq: 0, Ack: 1, Len: 1
Source Port: 50168
Destination Port: 80
[Stream index: 0]
[Stream Packet Number: 2]
[Conversation completeness: Incomplete (12)]
[TCP Segment Len: 1]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1919730549
[Next Segment Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 4166365118
0000 45 00 00 29 47 73 40 00 80 06 00 00 7f 00 00 01
0010 7f 00 00 01 c3 f8 00 50 72 6c c3 75 f8 55 af be
0020 50 10 27 b1 e7 e0 00 00 00
No.: 2 · Time: 0.000000 · Source: 127.0.0.1 · Destination: 127.0.0.1 · Protocol: HTTP · Length: 41 · Info: [TCP Spurious Retransmission] Continuation
Show packet bytes
Layout: Vertical (Stacked)
Help
Close


Wireshark · Packet 62 · test.pcap
[SEQ/ACK analysis]
[Bytes in flight: 6136]
[Bytes sent since last PSH flag: 6136]
[TCP Analysis Flags]
TCP payload (6136 bytes)
Hypertext Transfer Protocol
HTTP/1.1 401 Unauthorized\r\n
Cache-Control: private\r\n
Content-Type: text/html; charset=utf-8\r\n
Server: Microsoft-IIS/10.0\r\n
0000 45 00 18 20 47 af 40 00 80 06 00 00 7f 00 00 01
0010 7f 00 00 01 00 50 c3 f8 f8 55 df ae 72 6c c8 11
50 18 27 f1 6a f2 00 00 48 54 54 50 2f 31 2e 31
20 34 30 31 20 55 6e 61 75 74 68 6f 72 69 7a 65
64 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c
3a 20 70 72 69 76 61 74 65 0d 0a 43 6f 6e 74 65
6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74
6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d
38 0d 0a 53 65 72 76 65 72 3a 20 4d 69 63 72 6f
73 6f 66 74 2d 49 49 53 2f 31 30 2e 30 0d 0a 44
61 74 65 3a 20 53 75 6e 2c 20 31 33 20 4f 63 74
20 32 30 32 34 20 31 32 3a 33 38 3a 31 30 20 47
4d 54 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67
74 68 3a 20 35 39 35 36 0d 0a 0d 0a 3c 21 44 4f
43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49
43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58
48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f
Internet Protocol Version 4 (ip), 20 bytes


Wireshark · Packet 1 · test.pcap
Total Length: 52
Identification: 0x4774 (18292)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 127.0.0.1
Destination Address: 127.0.0.1
[Stream index: 0]
Transmission Control Protocol, Src Port: 80, Dst Port: 50168, Seq: 1, Ack: 1, Len: 0
Source Port: 80
0000 45 00 00 34 47 74 40 00 80 06 00 00 7f 00 00 01
0010 7f 00 00 01 00 50 c3 f8 f8 55 af be 72 6c c3 76
0020 80 10 27 f6 45 bf 00 00 01 01 05 0a 72 6c c3 75
0030 72 6c c3 76
Flags (ip.flags), 3 bits
Show packet bytes
Layout:
Vertical (Stacked)
Help
Close


IIS 10.0 Detailed Error - 401.3 - Una
IIS Windows
127.0.0.1
Windows
Internet Information Services
Welcome
Bienvenue
Tervetuloa
ようこそ
Benvenuto
歡迎
Bienvenido
Hoş geldiniz
ברוכים הבאים
Welkom
Bem-vindo
Vítejte
Καλώς ορίσατε
Välkommen
환영합니다
Добро пожаловать
Üdvözöljük
مرحبا
欢迎



HTTP Error 500.19 - Internal Server Error

The requested page cannot be accessed because the related configuration data for the page is invalid.

Detailed Error Information:

Module	IIS Web Core	**Requested URL**	http://www.kiyantube.com:80/
Notification	Unknown	**Physical Path**	
Handler	Not yet determined	**Logon Method**	Not yet determined
Error Code	0x80070005	**Logon User**	Not yet determined
Config Error	Cannot read configuration file due to insufficient permissions		
Config File	\\?\C:\Users\Windows\Desktop\New folder\web.config		

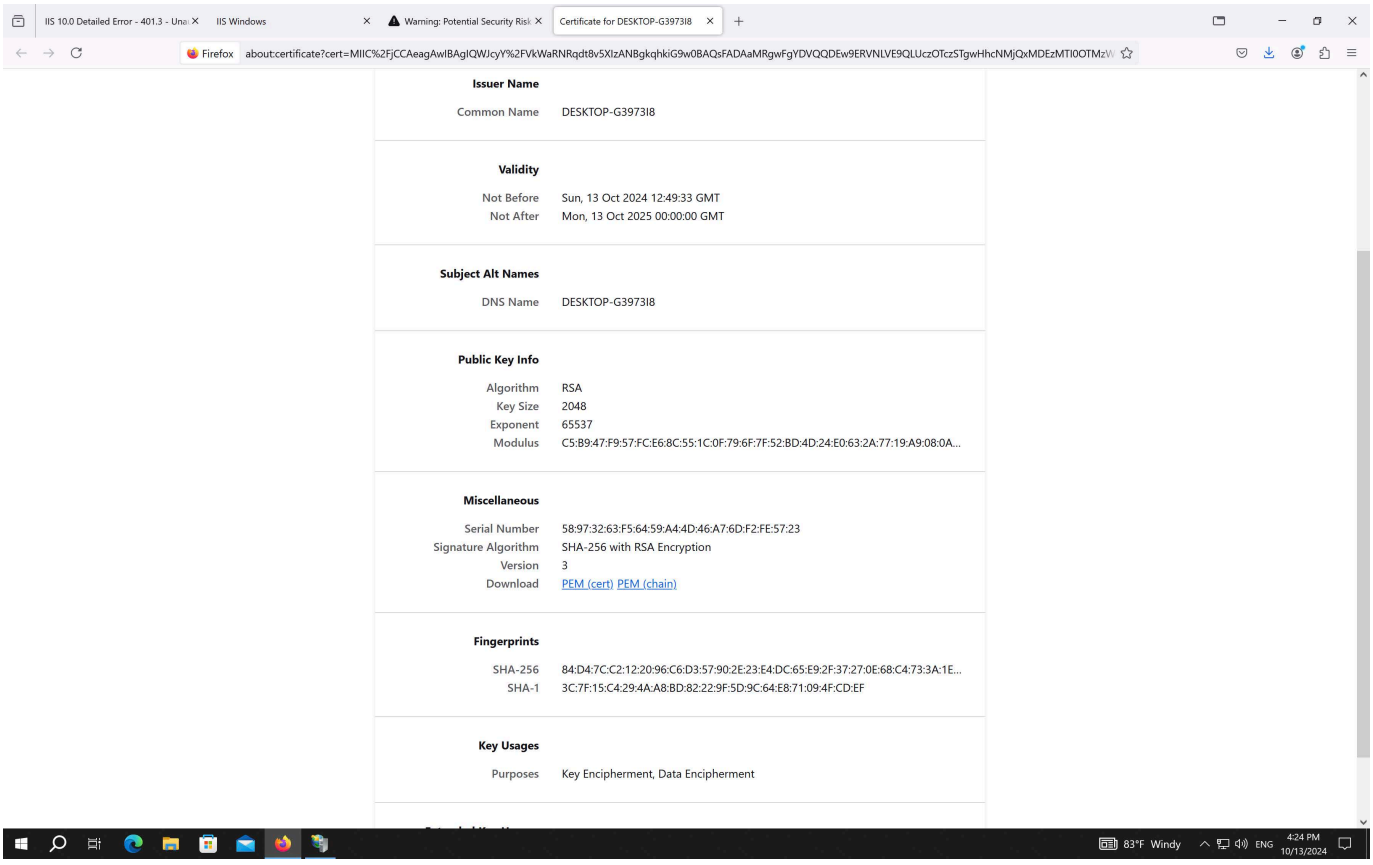
Config Source:

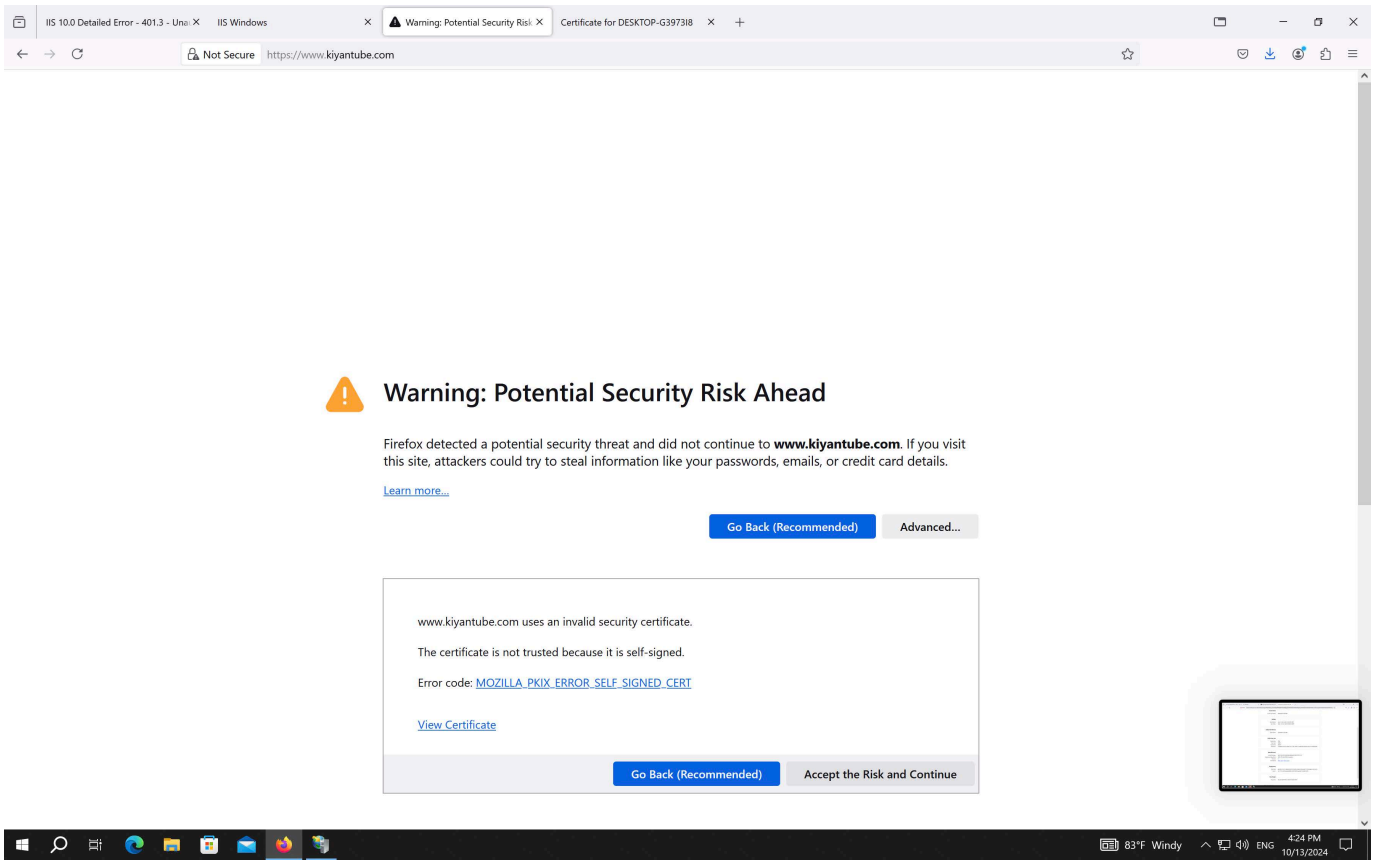
```
-1:
0:
```

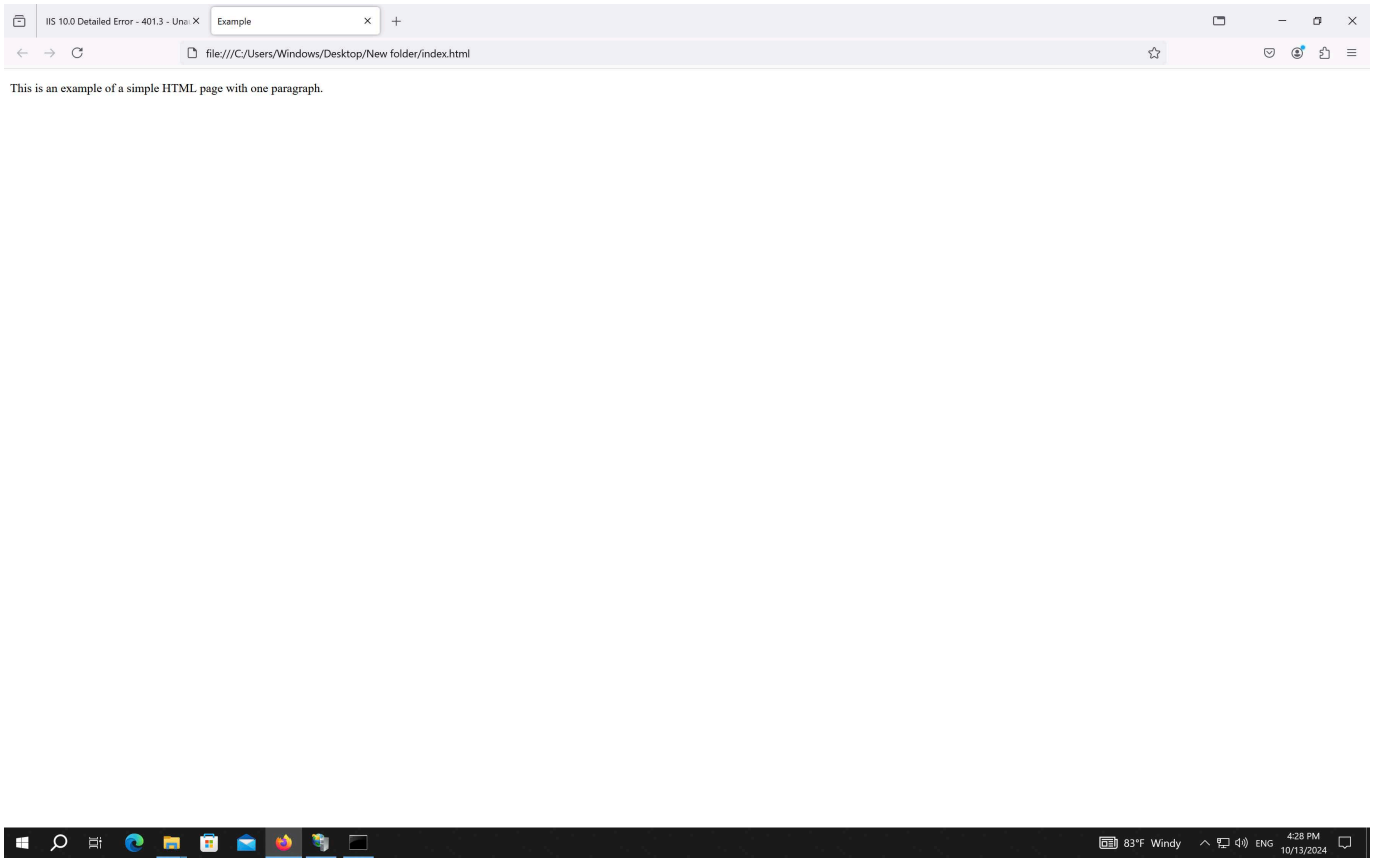
More Information:

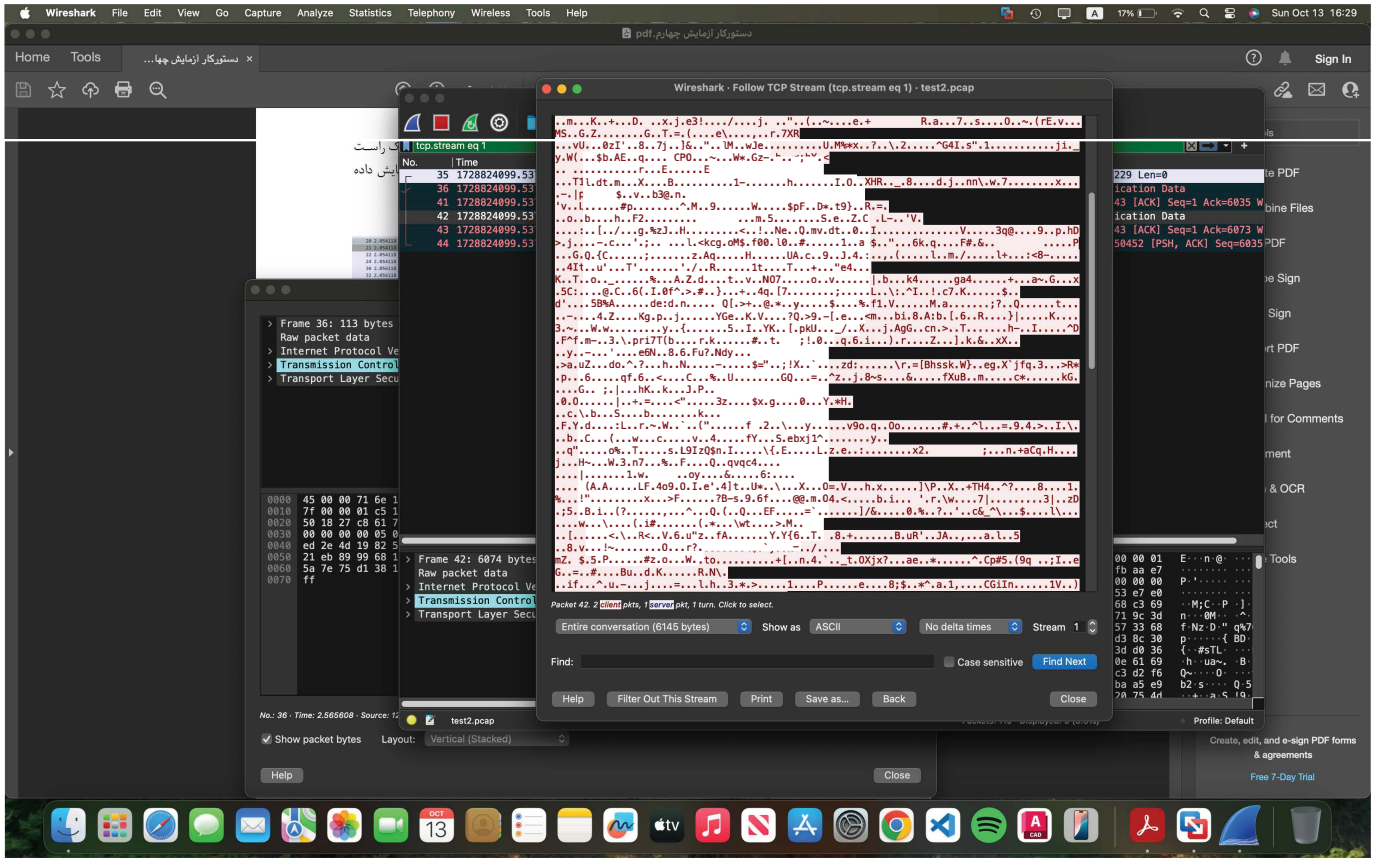
This error occurs when there is a problem reading the configuration file for the Web server or Web application. In some cases, the event logs may contain more information about what caused this error.

View more information »

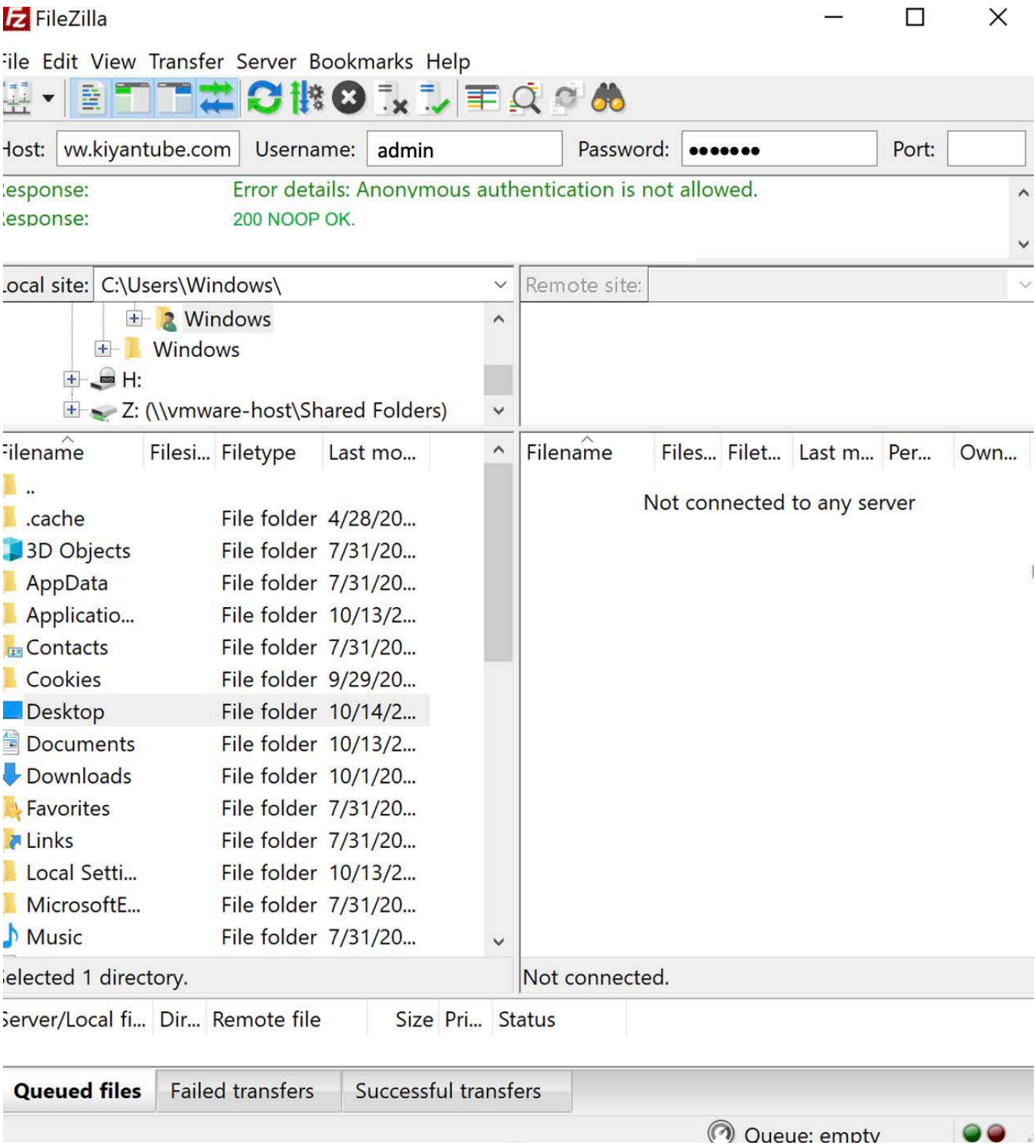



IIS 10.0 Detailed Error - 401.3 - Una
IIS Windows
Warning: Potential Security Risk
Certificate for DESKTOP-G3973I8
Not Secure
https://www.kiyantube.com
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to www.kiyantube.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
Learn more...
Go Back (Recommended)
Advanced...
www.kiyantube.com uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT
View Certificate
Go Back (Recommended)
Accept the Risk and Continue
83°F Windy
ENG
4:24 PM
10/13/2024


IIS 10.0 Detailed Error - 401.3 - Una
Example
file:///C:/Users/Windows/Desktop/New folder/index.html
This is an example of a simple HTML page with one paragraph.
83°F Windy
ENG
4:28 PM
10/13/2024



Hello this is Kiyan Tube ☺


FileZilla
File Edit View Transfer Server Bookmarks Help
Host: vw.kiyantube.com
Username: admin
Password: ●●●●●●
Port:
Response: Error details: Anonymous authentication is not allowed.
Response: 200 NOOP OK.
Local site: C:\Users\Windows\
Remote site:
Windows
Windows
H:
Z: (\\vmware-host\Shared Folders)
Filename Filesi... Filetype Last mo...
.. File folder
.cache File folder 4/28/20...
3D Objects File folder 7/31/20...
AppData File folder 7/31/20...
Applicatio... File folder 10/13/2...
Contacts File folder 7/31/20...
Cookies File folder 9/29/20...
Desktop File folder 10/14/2...
Documents File folder 10/13/2...
Downloads File folder 10/1/20...
Favorites File folder 7/31/20...
Links File folder 7/31/20...
Local Setti... File folder 10/13/2...
MicrosoftE... File folder 7/31/20...
Music File folder 7/31/20...
Filename Files... Filet... Last m... Per... Own...
Not connected to any server
elected 1 directory.
Not connected.
Server/Local fi... Dir... Remote file Size Pri... Status
Queued files
Failed transfers
Successful transfers
Queue: empty