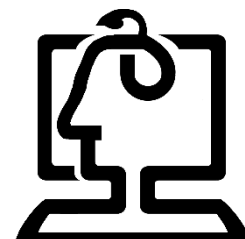


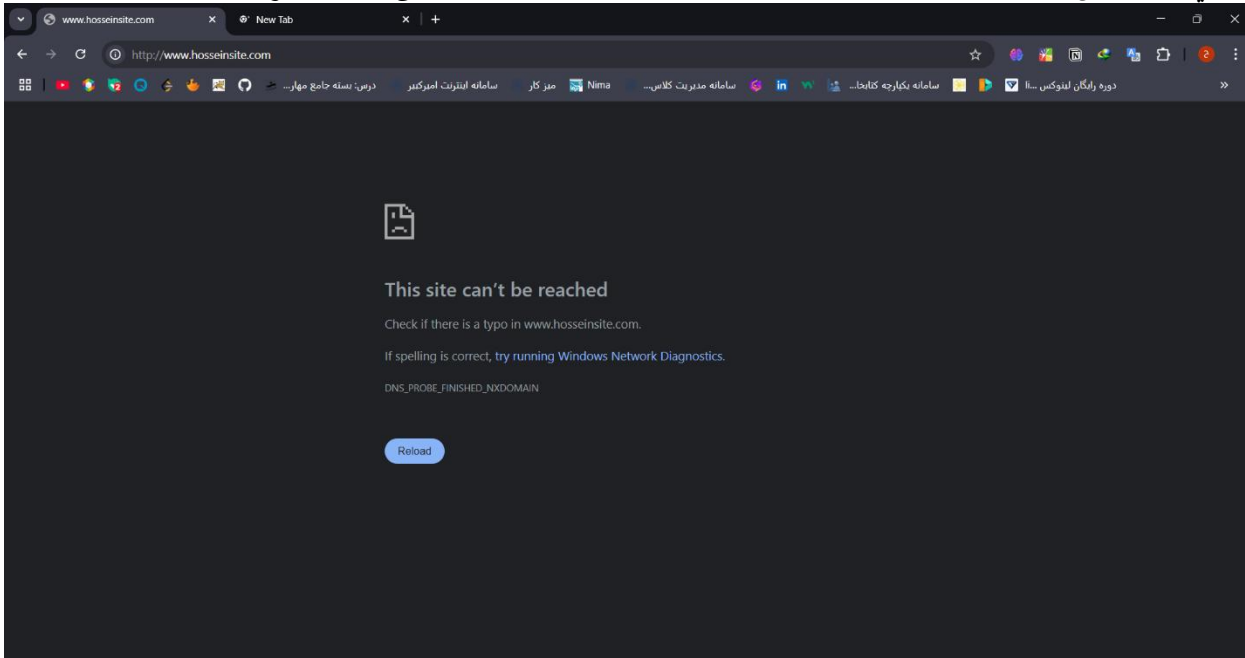


دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

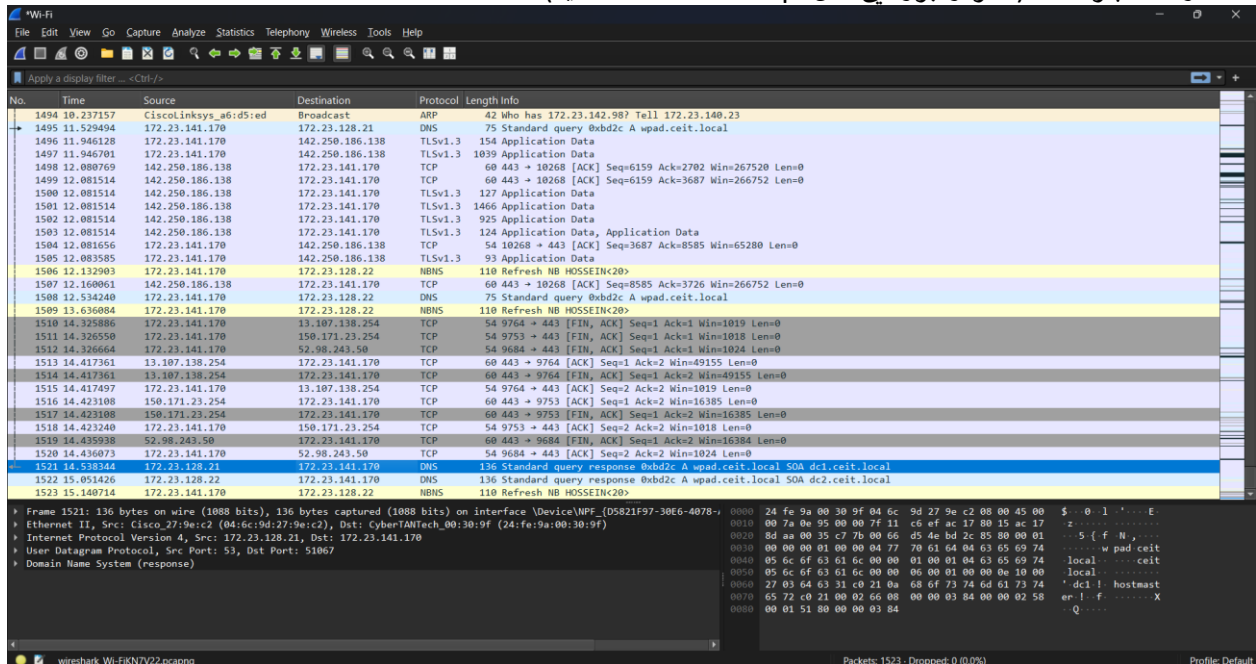


دانشکده مهندسی کامپیوتر

فرم گزارش کار آزمایشگاه شبکه

نام و نام خانوادگی	حسین تاتار	شماره دانشجویی	40133014	نام و شماره آزمایش	5 - راه اندازی سرویس های Web و FTP
هدف آزمایش	تنظیم سرور وب (IIS) - تجزیه و تحلیل ترافیک HTTP/HTTPS با ابزارهای Wireshark و RawCap راه اندازی سرویس FTP و بررسی امنیت ارتباطات				
ابزارهای مورد نیاز	Wireshark/RawCap برای تحلیل ترافیک شبکه FileZilla برای تست FTP IIS Manager برای مدیریت سرویس ها				
شرح آزمایش	<p>سوال 1: چرا سایت ایجاد شده در مرورگر نمایش داده نمی شود؟ جواب: عدم تنظیم صحیح رکورد DNS محلی فایل hosts : در ویندوز، آدرس www.hosseinsite.com باید به 127.0.0.1 یا IP سرور محلی نگاشت شود.</p>  <p>سوال 2: آدرس سایت خود را در مرورگر وارد کنید و ارتباط خود را با استفاده از Wireshark شنود کنید. آیا میتوانید مشخص کنید کدام بسته مربوط به سایت شما است؟ چه اتفاقی افتاده است؟ جواب: در تصویر، ترافیک عمدتاً مربوط به آدرس های 172.23.141.179 (کلاینت) و 142.20.16.18 (سرور خارجی) است و هیچ بسته ای با آدرس 127.0.0.1 یا www.hosseinsite.com دیده نمی شود.</p>				

علت ان اینست که اگر سایت شما روی 127.0.0.1 (لوکال هاست) اجرا شده باشد Wireshark به طور پیش فرض ترافیک لوکال هاست را غیرقابل مشاهده می کند. بسته های فرستاده شده به این آدرس هرگز به شبکه نمیروند بلکه تنها در داخل NIC در حال چرخشند (مگر از ابزارهایی مثل RawCap استفاده کنید).



سوال 3: آدرس پورتهای مبدأ و مقصد چیست؟ روند برقراری ارتباط در پروتکل HTTP چگونه است؟ وب سرور چگونه آدرس سایت درخواستی شما را تشخیص میدهد؟

جواب: پورت مبدأ 80 است و پورت مقصد 11264 میباشد.

روند برقراری ارتباط در پروتکل HTTP:

1 - شروع ارتباط:

• کلاینت: کلاینت، که معمولاً مرورگر وب است، به سرور وب درخواست میدهد. این درخواست شامل یک URL است که نشان میدهد کلاینت قصد دسترسی به چه منابعی را دارد.

• سرور: سرور وب، در نقش پاسخ دهنده، منتظر درخواستهای کلاینت میماند. این درخواستها از طریق پروتکل HTTP به سرور ارسال میشوند.

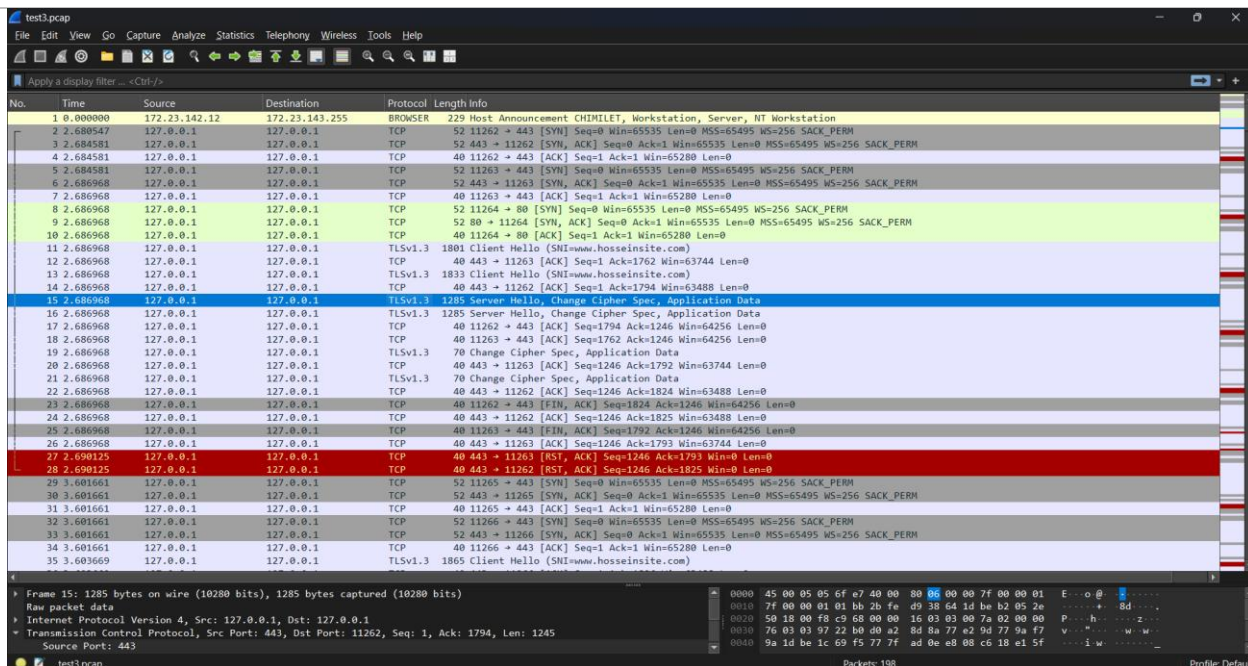
2 - ایجاد یک اتصال TCP:

از پروتکل TCP/IP برای برقراری ارتباط استفاده میکند. بنابراین، کلاینت ابتدا یک اتصال TCP به سرور ایجاد کند که شامل برقراری ارتباط با سرور (کلاینت با استفاده از آدرس IP سرور و پورت مناسب معمولاً پورت 80 برای HTTP و پورت 443 برای HTTPS یک اتصال TCP ایجاد میکند.) و مرحله دستیابی به سرور (مرورگر یا کلاینت، URL مورد نظر را به یک آدرس IP تبدیل میکند و سپس درخواست خود را به سرور ارسال میکند).

3 - ارسال درخواست HTTP: پس از برقراری اتصال، TCP کلاینت یک درخواست HTTP به سرور ارسال میکند.

4 - دریافت و پردازش درخواست توسط سرور: پس از دریافت درخواست، سرور آن را پردازش میکند.

5 - ارسال پاسخ HTTP: سرور پس از پردازش درخواست، یک پاسخ HTTP به کلاینت ارسال میکند

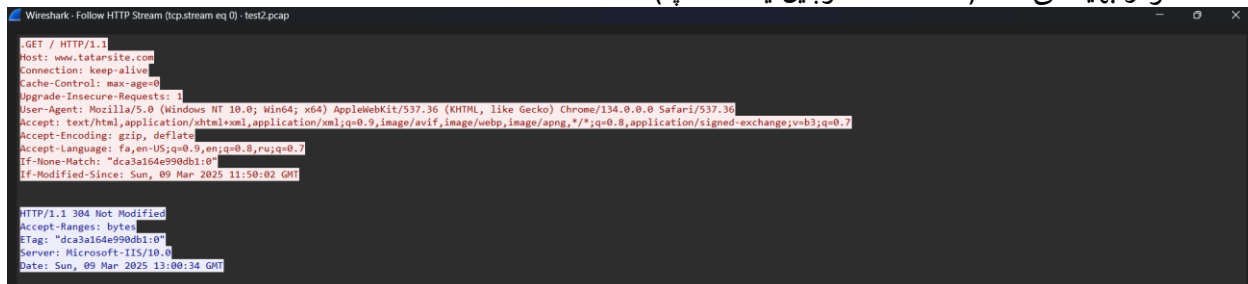


سوال 4: مقدار بخش Connection چیست؟ درخواست HTTP از نوع GET بوده است یا از نوع POST؟ مقدار User-Agent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟

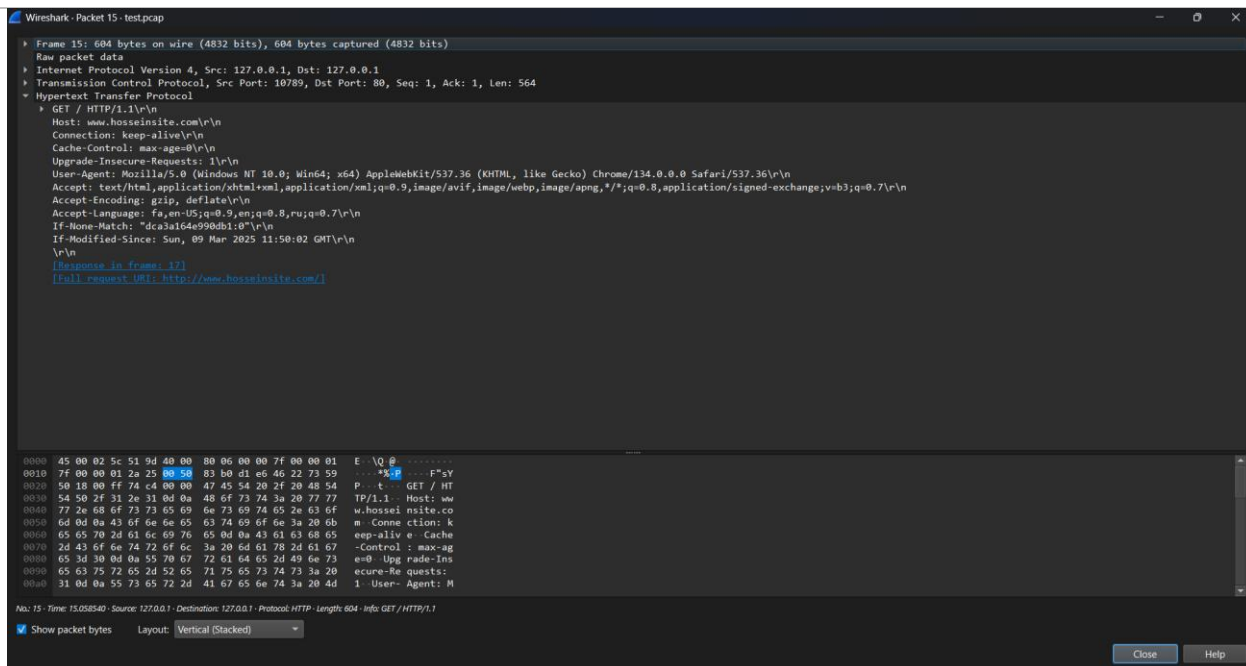
جواب: مقدار بخش Connection برابر keep-alive است، به این معنی که کلاینت از سرور میخواهد کانکشن TCP را حتی بعد از اتمام درخواست اولیه باز نگه دارد. درخواست از نوع GET است، به این معنی که کلاینت درخواست دریافت یک resource از سرور را دارد. مقدار User-Agent نیز برابر:

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.58 Safari/537.36

- مرورگر Google Chrome: نسخه ۹۳.۰.۴۵۷۷.۵۸.
 - سیستم عامل: Windows 10 (64-bit)
 - موتور رندرینگ: AppleWebKit (مشترک بین Safari و Chrome)
- این رشته نشان می‌دهد کلاینت از Chrome روی ویندوز استفاده کرده است. برخی سایت‌ها بر اساس محتوا را بهینه می‌کنند (مثلاً نسخه موبایل یا دسکتاپ).



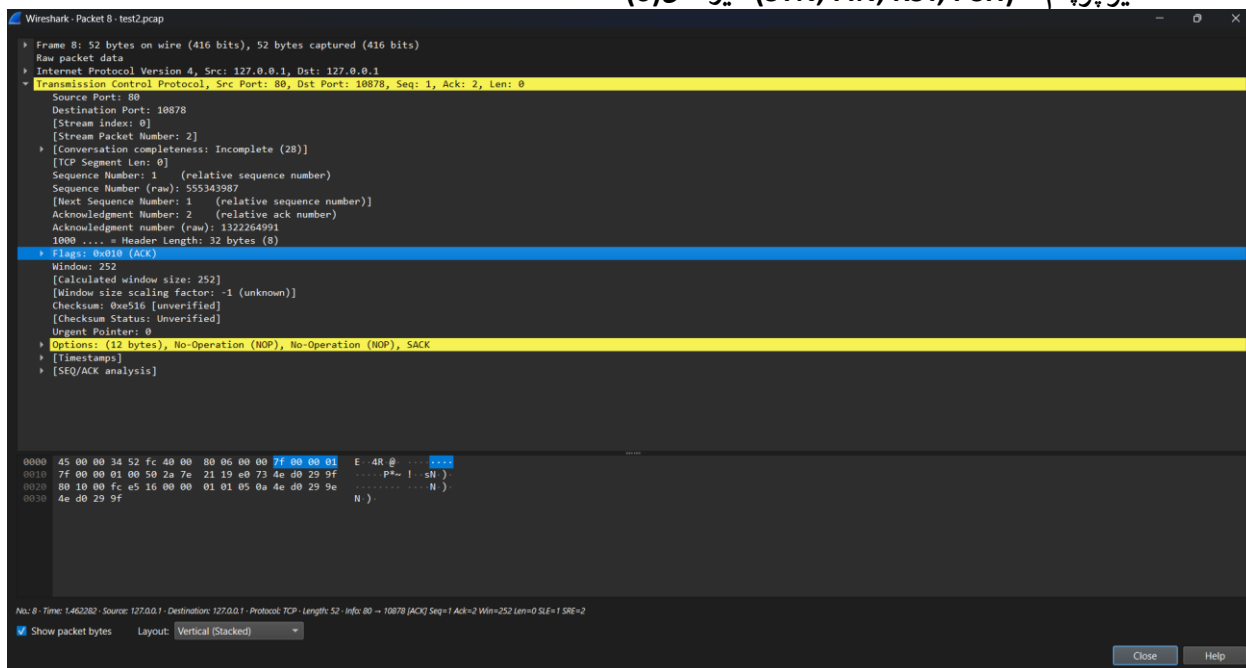
عکس مشاهده شده توسط نرم افزار Wireshark :



سوال 5: در پنجره باز شده، اولین بسته را انتخاب کنید. سپس مقدار Flags در پروتکل TCP را مشاهده کنید. چه مقادیری برای این بسته تنظیم شده است؟

جواب: کد هگز (0x010) نشان دهنده‌ی فعال بودن فقط پرچم ACK در این بسته است.

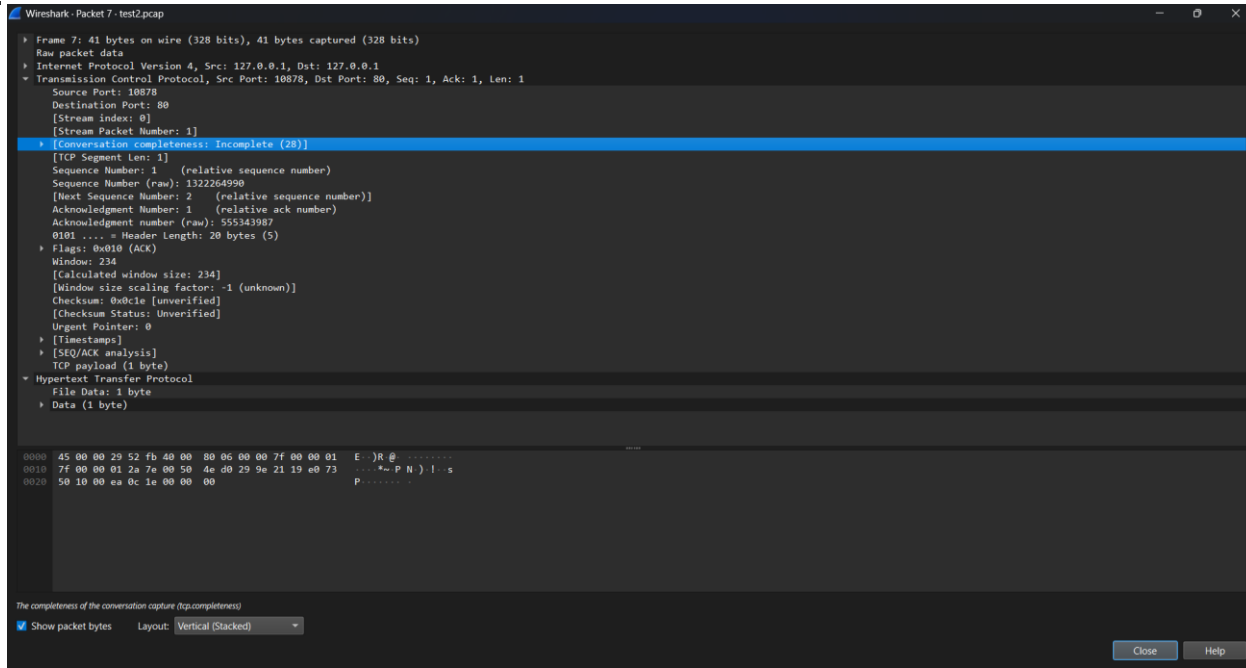
- **ACK (Acknowledgment) فعال (1)**
- تأیید دریافت داده‌های قبلی توسط گیرنده.
- **سایر پرچم‌ها (SYN, FIN, RST, PSH) غیرفعال (0)**



سوال 6: یک سایت دیگر با نام دلخواه ایجاد کنید و بسته‌های مربوط به آن را شنود کنید. چه تفاوتی بین این دو سایت وجود دارد؟

جواب: تفاوت این دو سایت شامل:

- 1 - هدر Host در HTTP : سرور بر اساس این هدر تشخیص می دهد کدام سایت را نمایش دهد.
- 2 - محتوای بسته ها : داده های منتقل شده متفاوت هستند (به خاطر فایل های مختلف)
- 3 - گواهی SSL در صورت استفاده از HTTPS : هر سایت گواهی مخصوص به خود دارد (حتی اگر خودامضا باشد)
- 4 - پورت های استفاده شده : اگر پورت ها متفاوت باشند، ترافیک در Wireshark با پورت های مختلف فیلتر می شود.



سوال 7: درمرورگر آدرس 127.0.0.1 را تایپ کنید. چرا هیچکدام از سایتها نمایش داده نمیشوند؟

جواب: مکانیسم تشخیص سایت در IIS :

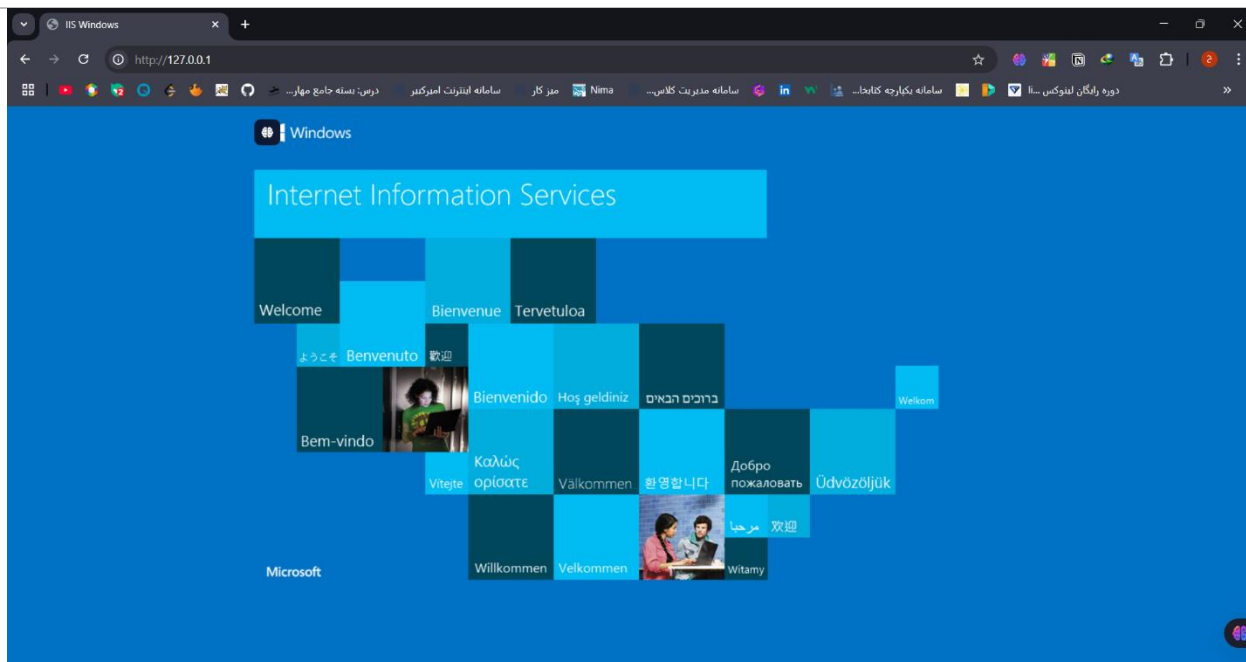
وب سرور IIS از هدر Host در درخواست HTTP برای تشخیص سایت درخواستی استفاده می کند.

وقتی آدرس 127.0.0.1 را مستقیماً وارد می کنیم، مرورگر هدر Host را ارسال نمی کند یا آن را به صورت Host: 127.0.0.1 ارسال می کند.

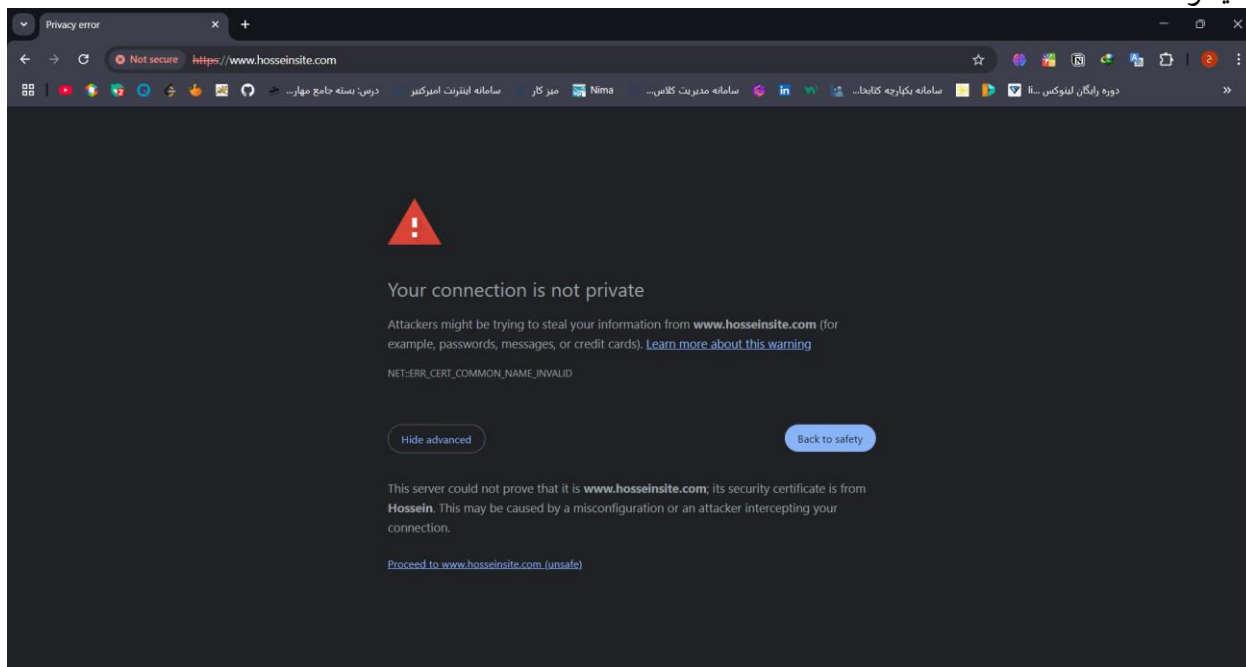
از آنجا که سایت های ما با Hostname های خاص مثل www.hosseinsite.com یا www.test2.com تنظیم شده اند IIS نمی تواند مطابقت صحیحی پیدا کند.

در نتیجه عدم نمایش سایت ها به دلیل تنظیم نشدن Hostname در درخواست مرورگر و عدم تطابق با Binding های تعریف شده در IIS است.

در تصویر زیر، پیام "Welcome" نشان دهنده ی صفحه پیش فرض IIS است (نه سایت های ایجاد شده توسط ما).

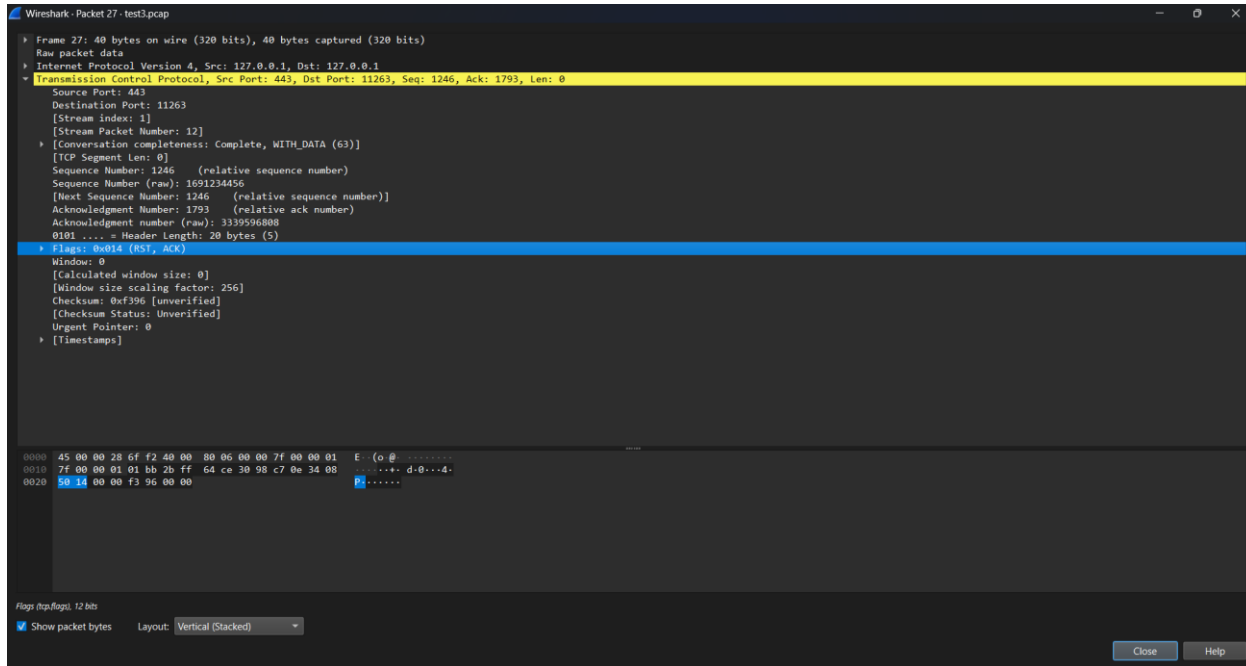


آدرس سایت دوم را (<https://www.hosseinsite.com>) را در مرورگر باز میکنیم.
سوال 8: آیا با مشکلی مواجه شدید؟ اگر بله است با استفاده از rawcap مشخص کنید که چه مشکلی وجود دارد.
جواب: بله - مشکل اصلی عدم تطابق نام دامنه در گواهی SSL است. در ابتدا درخواست اتصال فرستاده میشود و مرورگر یک key برمیگرداند و از آنجایی که key ای که توسط مرورگر فرستاده شده با key موجود یکسان نمیباشد اتصال امن برقرار نمیشود.



حال با استفاده از عکس زیر میتوان مشاهده کرد که :
 - عدم نمایش Handshake کامل TLS : در تصویر، بخش‌های کلیدی مثل Client Hello یا Server Hello دیده نمی‌شوند که معمولاً در آنها نام دامنه و گواهی SSL مبادله می‌شود. این ممکن است به دلیل قطع شدن ارتباط یا خطا در مرحله Handshake باشد.

- پنجره (Window Size) صفر است : مقدار Window: 0 ممکن است نشان‌دهنده قطع ارتباط یا مشکل در ارسال داده باشد (مثلاً به دلیل رد گواهی توسط کلاینت)
- پورت 443 فعال است : نشان می‌دهد سرور در حال شنیدن درخواست‌های HTTPS است، اما ممکن است گواهی نادرست ارائه دهد.



سوال 9: مشخص کنید که گواهی را چه کسی برای چه کسی صادر کرده، مدت زمان اعتبارگواهی چه قدر است. کلید عمومی صادرکننده چیست و امضای دیجیتال انجام شده با چه الگوریتم هایی انجام شده است.

جواب: با توجه به تصاویر زیر مشاهده میکنیم که:

گواهی برای سروری که همان لپتاپ خودم هست صادر شده است در واقع توسط دسکتاپ خودم برای همین دسکتاپ تولید شده است (Hossein).

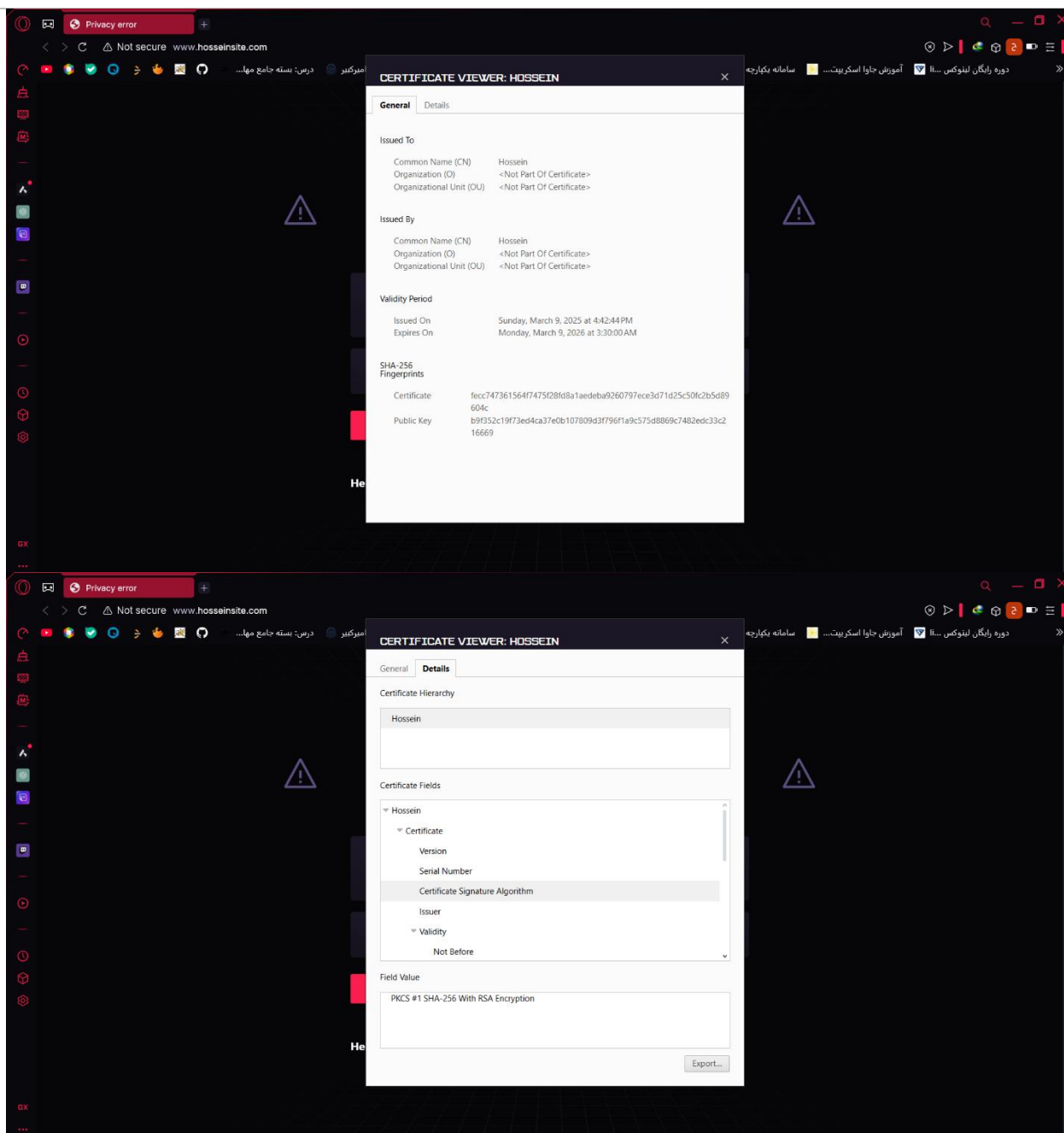
مدت اعتبار آن از ۹ مارس ۲۰۲۵ ساعت ۱۶:۴۲ تا ۱۰ مارس ۲۰۲۶ ساعت ۳:۳۰ به اندازه یک سال است.

کلید عمومی صادرکننده آن به صورت روبرو است :

b9f352c19f73ed4ca37e0b107809d3f796f1a9c575d8869c7482ecdc33c216669

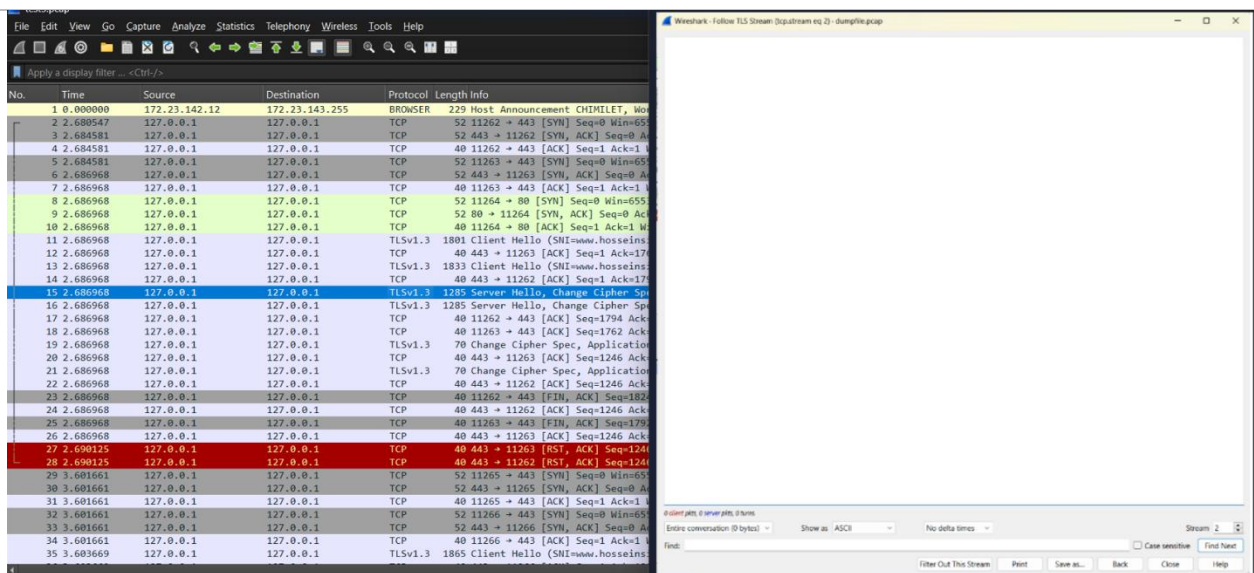
الگوریتم‌های امضای دیجیتال آن :

- Fingerprint برای SHA-256
- RSA با توجه به ساختار استاندارد گواهی‌های خودامضا



سوال 10: آیا میتوانید متن ارتباط را بخوانید؟ چرا؟

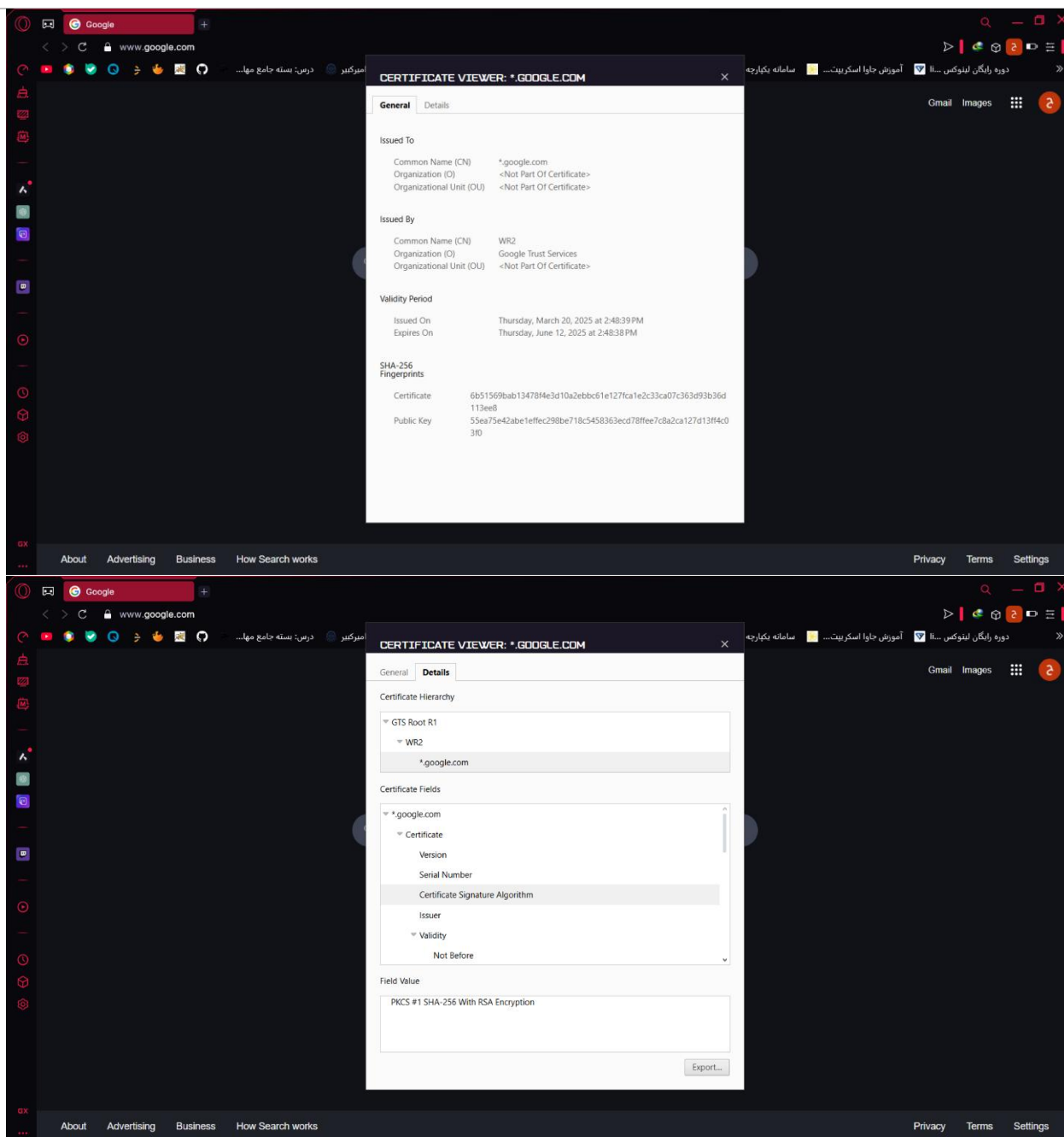
جواب: پروتکل TLS/SSL تمام داده‌های مبادله‌شده را رمزنگاری می‌کند. حتی با ابزارهایی مثل Wireshark یا RawCap، بدون دسترسی به کلید خصوصی سرور، نمی‌توان محتوای اصلی را مشاهده کرد.



سوال 11: به یک سایت مانند <https://www.google.com> وصل شده، گواهی آن را بررسی کنید. گواهی آن سایت با گواهی سایت شما چه تفاوت هایی دارد؟

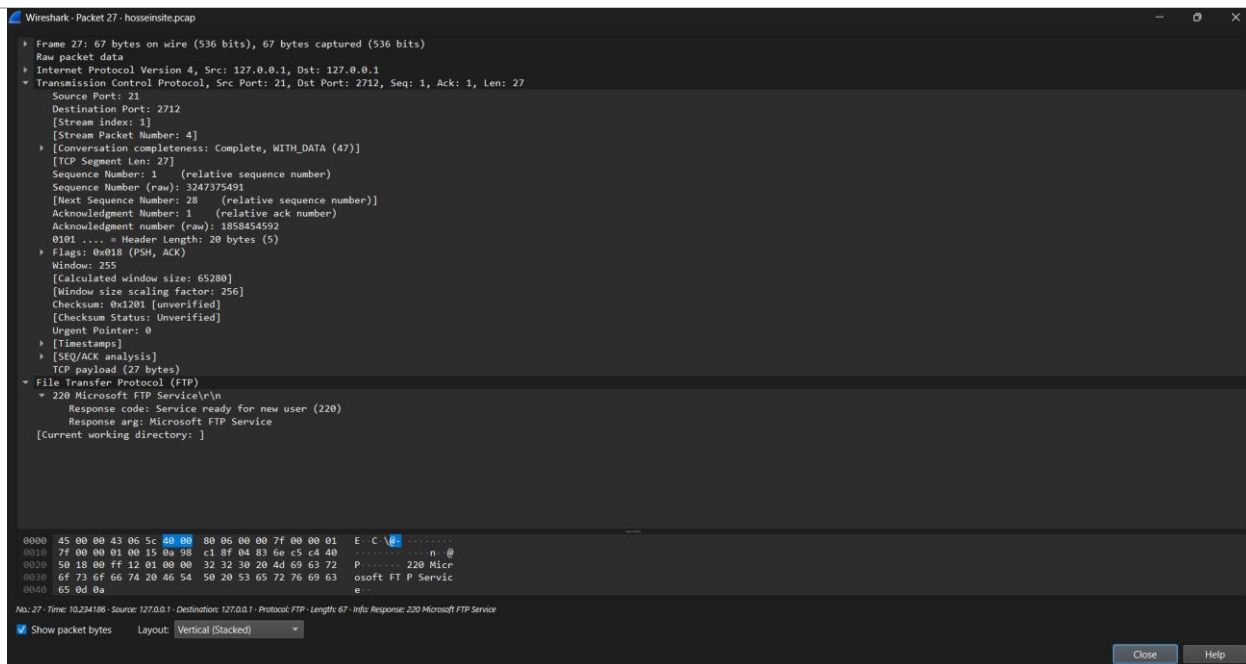
جواب:

توضیح	گواهی آزمایشگاه شما (Hossein)	گواهی (*.google.com) Google	معیار مقایسه
گواهی Google توسط یک CA معتبر صادر شده، اما گواهی شما خودساخته است.	خودامضا (صادرکننده و دریافت کننده یکسان) Hossein :	Google Trust Services مرجع معتبر جهانی	صادرکننده (Issuer)
گواهی Google برای دامنه های واقعی بهینه شده است.	بدون اشاره به دامنه خاص	پشتیبانی از زیردامنه ها با Wildcard	نام دامنه (CN/SAN)
مروورگها به گواهی Google اعتماد می کنند، اما گواهی شما را رد می کنند.	فاقد اعتبارسنجی (Self-Signed)	Extended Validation (EV) یا Organization Validated (OV)	اعتبارسنجی
گواهی های معتبر معمولاً عمر کوتاه تری دارند.	۱ سال	۳ ماه مطابق استانداردهای جدید (CA)	مدت اعتبار
هر دو از الگوریتم های مدرن استفاده می کنند.	SHA-256 + RSA پایه	SHA-256 + RSA/ECC پیشرفته و امن	الگوریتم ها
گواهی Google برای استفاده در اینترنت طراحی شده است.	محلی/تستی (فقط برای محیط های توسعه)	عمومی (قابل اعتماد برای همه کاربران)	کاربرد



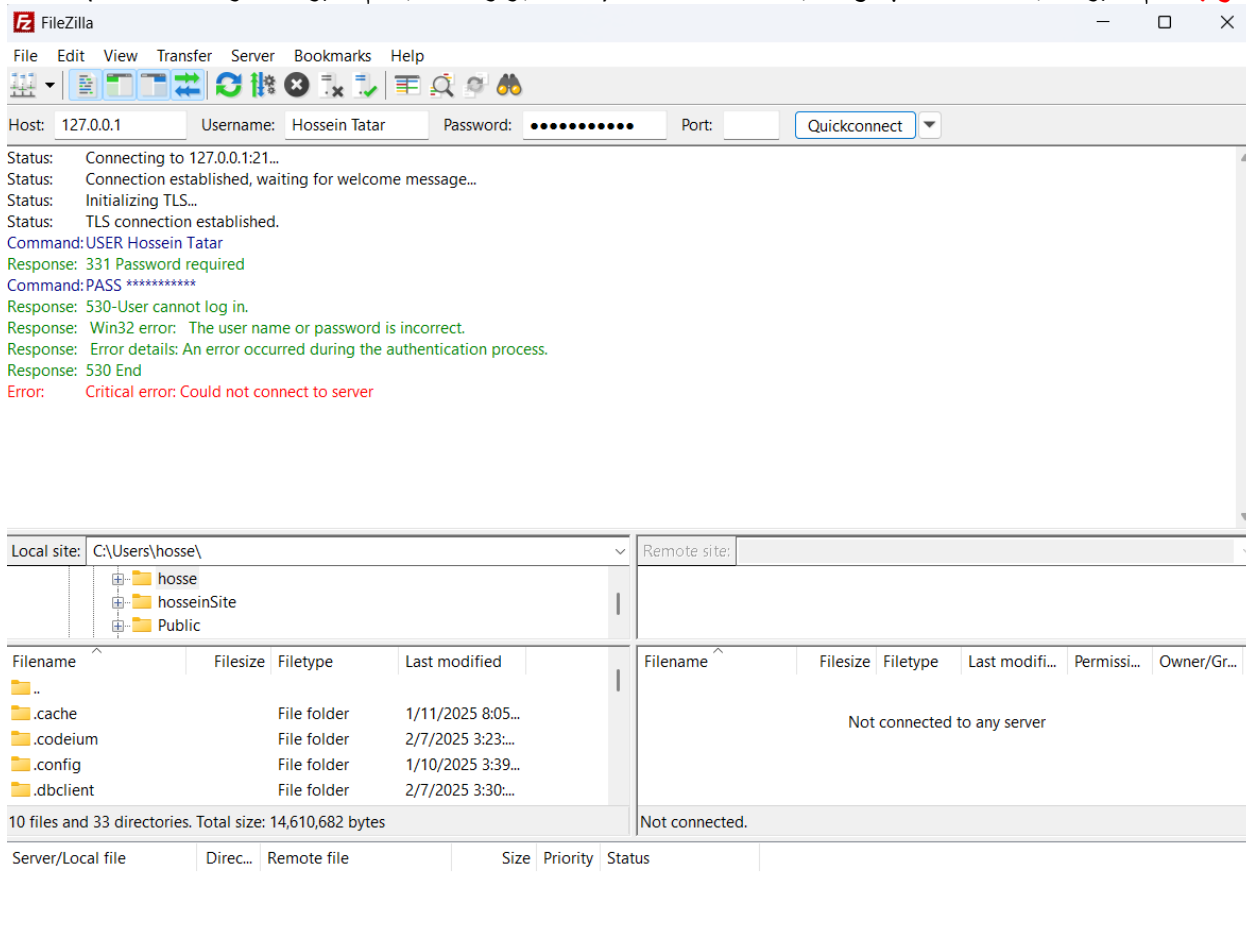
سوال 12: مشخص کنید چه دستوری برای لیست کردن فایل های دایرکتوری استفاده شده است. مشخص کنید چه نام کاربری برای دسترسی به سایت استفاده شده است. پروتکل لایه Transport استفاده شده برای این بسته ها چیست؟ آدرس پورت مبدا و مقصد ارتباط را مشخص کنید.

جواب: از دستور LIST برای لیست کردن دایرکتورها استفاده میشود. از طرفی چون در وضعیت ناشناس یا anonymously هستیم رمز و نام کاربری قابل مشاهده نیست همچنین پروتکل لایه انتقال TCP است. FTP از TCP به دلیل قابلیت اطمینان در انتقال داده استفاده می کند. پورت مبدا ۲۱ و پورت مقصد نیز 2712 است.

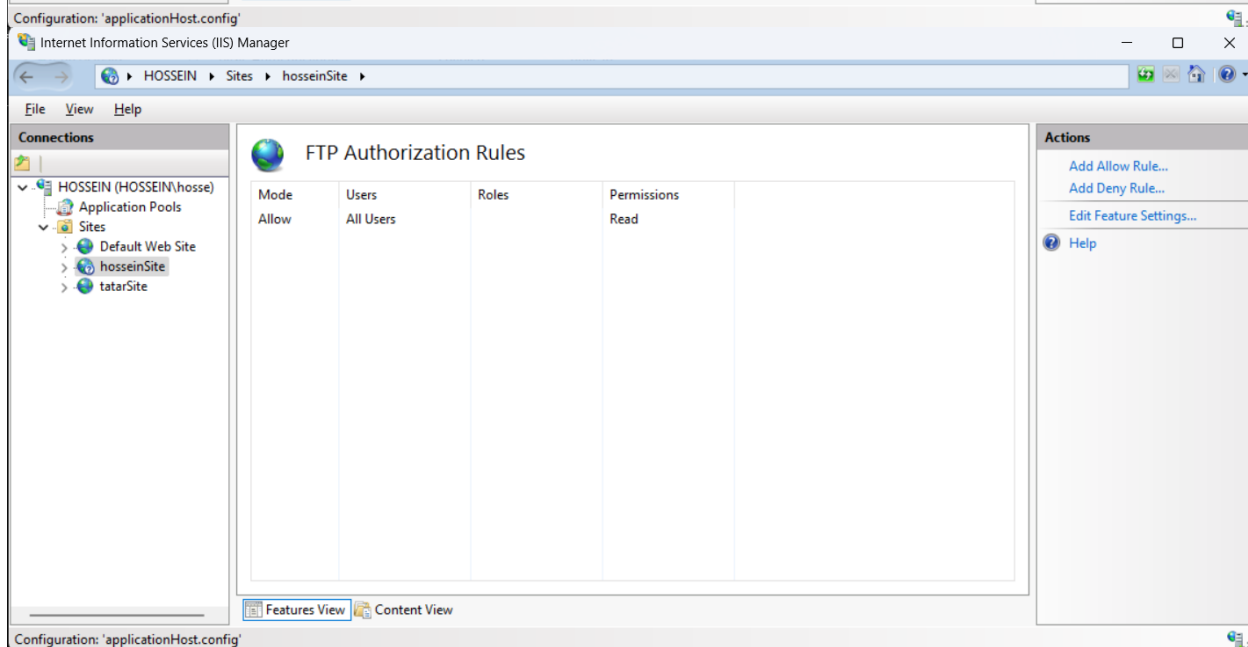
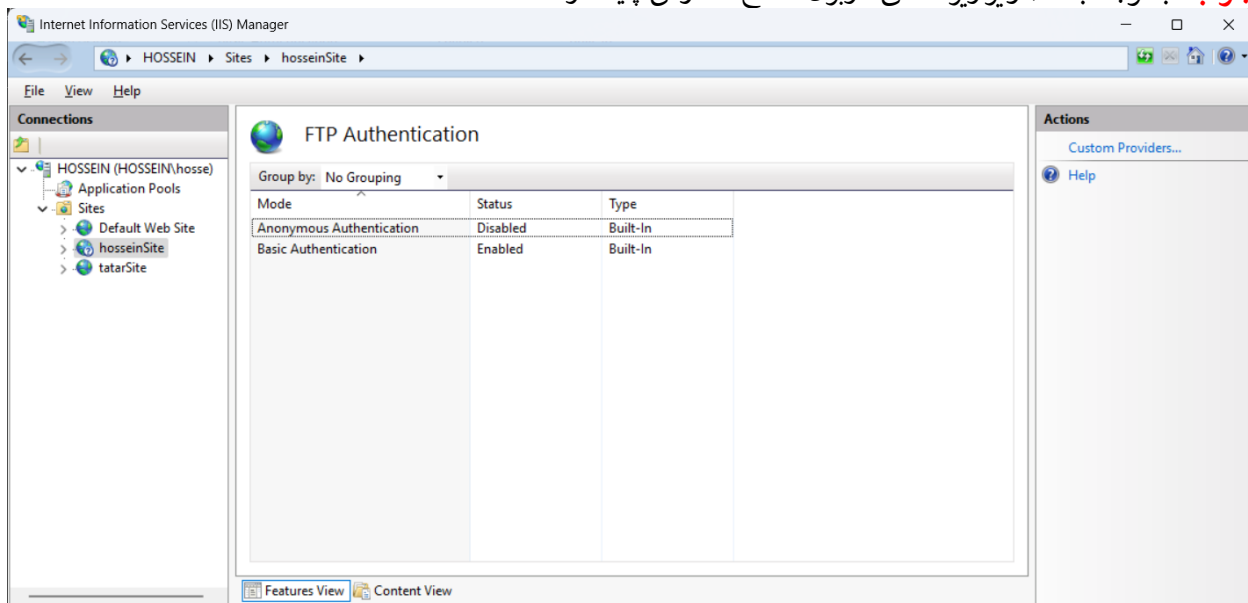


سوال 13: آیا نام کاربری و پسورد قابل خواندن است؟

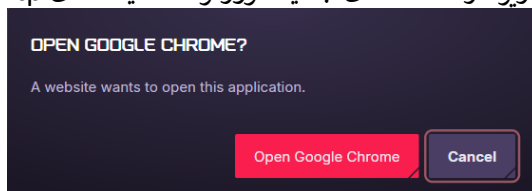
جواب: نام کاربری قابل مشاهده و پسورد قابل مشاهده نیست (اتصال برقرار نشد با نام کاربری و رمز های مختلف).



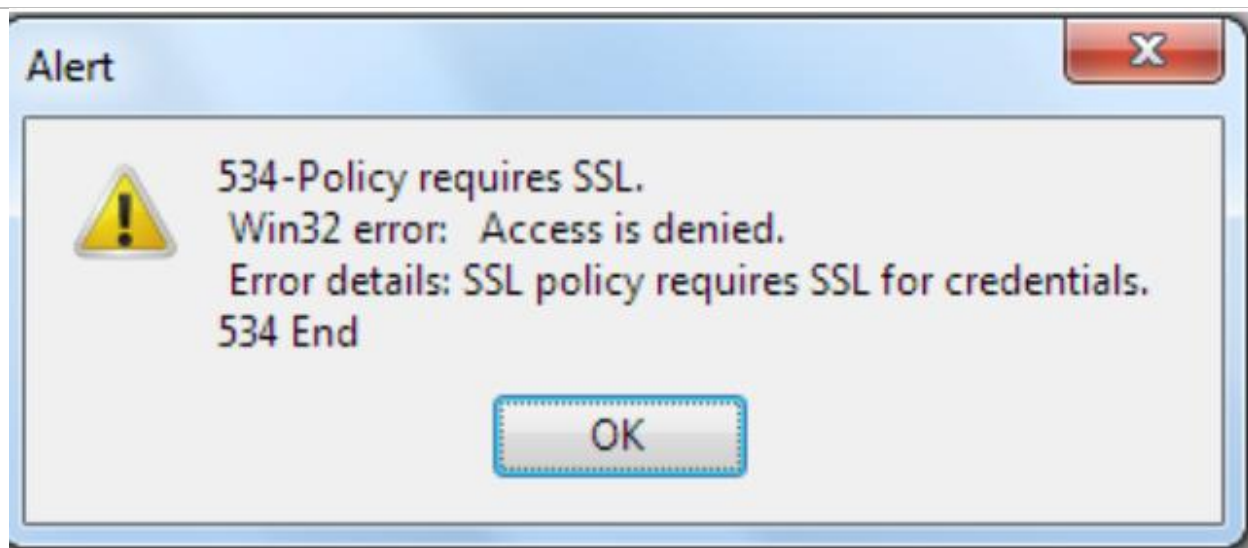
سوال 14: به FTP Authentication و FTP Authorization بروید و سطوح دسترسی را مشخص کنید.
جواب: با توجه به تصاویر زیر، تمامی کاربران سطح دسترسی پایه دارند.



سوال 15: سعی کنید دوباره سایت را از مرورگر باز کنید. آیا میتوانید به سایت وارد شوید؟
جواب: خیر نمیتوان وارد سایت شد زیرا در نسخه های جدید مرورگرها سایت های ftp را باز نمیکنند.



سوال 16: در مرورگر فایرفاکس خطای نمایش داده شده در شکل زیر نمایش داده میشود. معنی این خطا چیست؟



جواب: این خطا نشان می‌دهد سرور FTP شما تنظیمات امنیتی خاصی دارد که اجازه‌ی احراز هویت (ورود کاربر) بدون استفاده از SSL/TLS را نمی‌دهد.

پروتکل http

جواب: این بخش برای من با مشکل مواجه شده است.

پروتکل ftp :

جواب اول: این بخش نیز برای من با مشکل مواجه شد.

