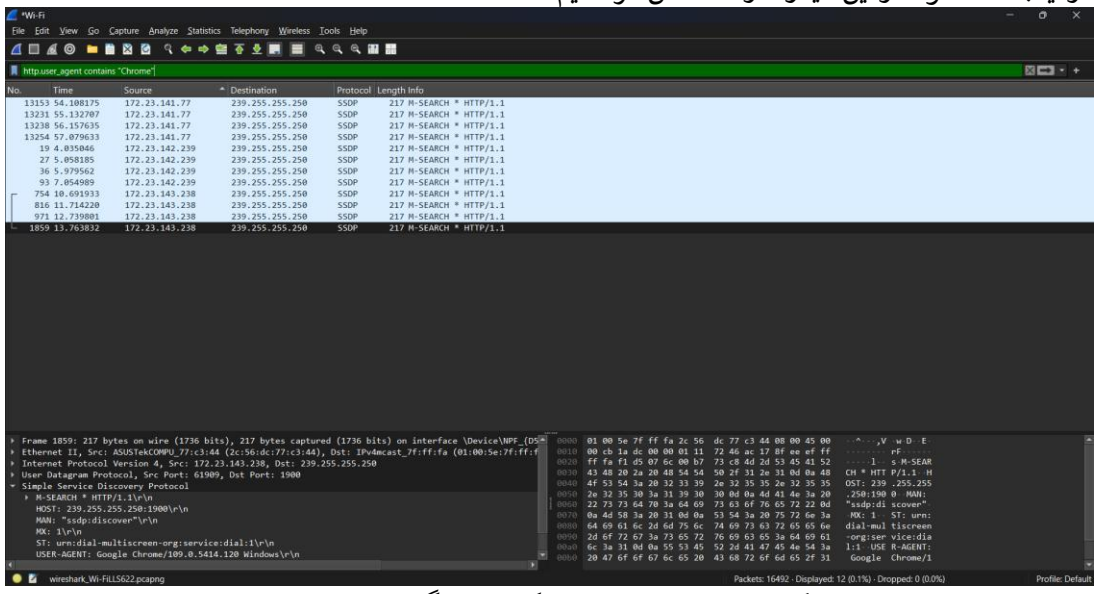
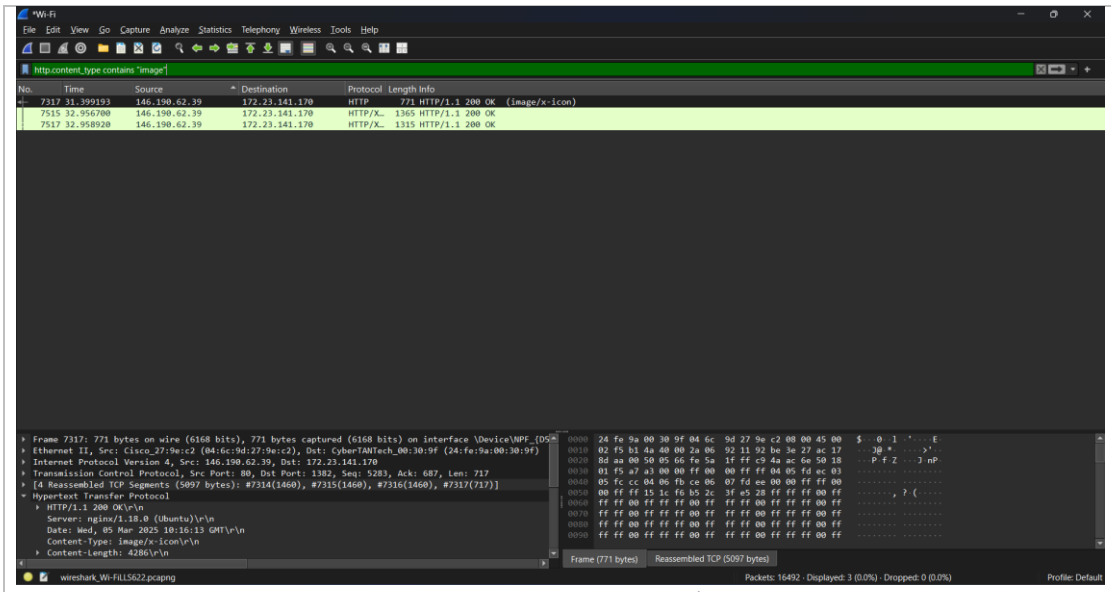
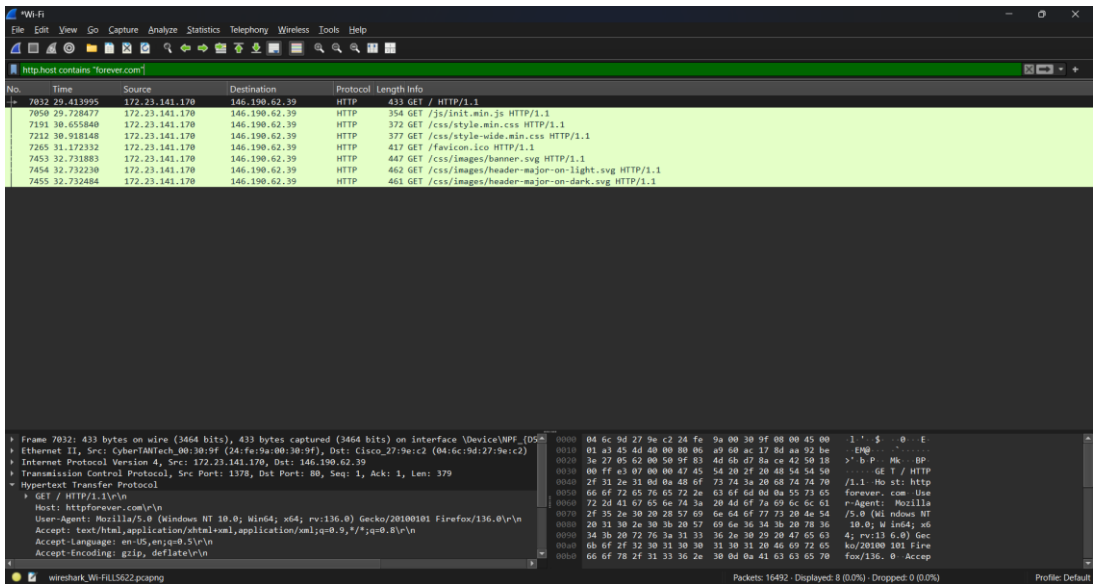
نام و نام خانوادگی	**حسین تاتار**	شماره دانشجویی	**40133014**	نام و شماره آزمایش	**4 - تحلیل http با استفاده از نرم افزار WireShark**
هدف آزمایش	چگونگی استفاده از Wireshark برای ضبط و تحلیل ترافیک HTTP برای درک ارتباطات وب، شناسایی مشکلات امنیتی احتمالی و بررسی ناهنجاریهای ترافیک شبکه				
ابزارهای مورد نیاز	نصب Wireshark روی سیستم شما یک مرورگر وب برای ایجاد ترافیک HTTP				
شرح آزمایش	**سوال 1:** چند نمونه از فیلترهای دیگر را مشخص کرده و توضیح دهید که برای چه کاری استفاده می شوند. **جواب:** در اینجا سه نمونه از این فیلتر هارا مشخص کرده ایم:  توضیح :این فیلتر فقط ترافیک HTTP را نشان می‌دهد که از مرورگر Chrome ارسال شده است. کاربرد :زمانی که می‌خواهید تحلیل کنید کدام کاربران از مرورگر Chrome استفاده می‌کنند.				



توضیح :این فیلتر فقط ترافیک HTTP را که شامل محتوای تصویری مانند JPEG, PNG و غیره نشان میدهد.
کاربرد :زمانی که می‌خواهید تحلیل کنید کدام تصاویر در حال بارگیری هستند.



توضیح :این فیلتر فقط ترافیک HTTP را نشان می‌دهد که مربوط به میزبان "forever.com" (Host) است.
کاربرد :زمانی که می‌خواهید فقط ترافیک مربوط به یک دامنه خاص را مشاهده کنید، مثلاً برای تحلیل ترافیک یک وب‌سایت خاص.

سوال 2: چند نمونه از هدرهای HTTP دیگر را بررسی و به طور کامل توضیح دهید.به طور مثال E-tag :

جواب:

Accept :

توضیح: این هدر مشخص می‌کند که کلاینت (مرورگر) چه نوع محتوایی را می‌تواند دریافت کند. این می‌تواند شامل انواع MIME مانند text/html، application/jsonو غیره باشد.

مثال Accept :

text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Language :

توضیح: این هدر زبان‌های ترجیحی کلاینت را مشخص می‌کند. سرور می‌تواند از این اطلاعات برای ارائه محتوای مناسب به زبان مورد نظر استفاده کند.

مثال Accept-Language :

en-US,en;q=0.5

Authorization :

توضیح: این هدر برای ارسال اطلاعات احراز هویت به سرور استفاده می‌شود. این می‌تواند شامل توکن‌های Bearerیا اطلاعات پایه مانند نام کاربری و رمز عبور باشد.

مثالAuthorization :

Bearer <token>

ETag :

توضیح: ETag مخفف (Entity Tag) یک هدر HTTP است که برای مدیریت کش (Cache) و اعتبارسنجی منابع استفاده می‌شود. این هدر توسط سرور به یک منبع (مانند یک فایل، تصویر، یا صفحه وب) اختصاص داده می‌شود و به کلاینت (مرورگر یا کاربر) اجازه می‌دهد تا بررسی کند که آیا نسخه‌ای از منبع که در کش ذخیره شده است، هنوز معتبر است یا خیر.

مثال ETag :

ETag: "63754f44-63"\r\n

سوال 3:کدهای 3x,4x,5x را با جزییات بررسی کرده و علت وقوع هرکدام را توضیح دهید.

جواب:

کدهای 3x (هدایت‌ها):

این کدها نشان‌دهنده این هستند که کلاینت باید اقدامات بیشتری انجام دهد تا درخواست را کامل کند. معمولاً این اقدامات شامل ریدایرکت (هدایت) به یک URL دیگر است.

1. 301 Moved Permanently:
   - توضیح :این کد نشان‌دهنده این است که منبع درخواست شده به طور دائم به یک URL جدید منتقل شده است.
   - علت وقوع :تغییر دائمی آدرس یک صفحه وب.
2. 302 Found:
   - توضیح :این کد نشان‌دهنده این است که منبع به طور موقت به یک URL جدید منتقل شده است.
   - علت وقوع :تغییر موقت آدرس یک صفحه وب.
3. 304 Not Modified:
   - توضیح :این کد نشان‌دهنده این است که منبع از زمان آخرین درخواست تغییر نکرده است و کلاینت می‌تواند از نسخه کش شده استفاده کند.
   - علت وقوع :استفاده از کش برای کاهش بار سرور و بهبود عملکرد.

کدهای 4x (خطاهای کلاینت):

این کدها نشان‌دهنده این هستند که خطایی در سمت کلاینت رخ داده است و سرور نمی‌تواند درخواست را پردازش کند.

1. 400 Bad Request:
   - توضیح :این کد نشان‌دهنده این است که درخواست کلاینت نامعتبر یا ناقص است.
   - علت وقوع :فرمت نادرست درخواست، پارامترهای نامعتبر.
2. 401 Unauthorized:
   - توضیح :این کد نشان‌دهنده این است که کلاینت باید خود را احراز هویت کند تا به منبع دسترسی پیدا کند.

- علت وقوع :عدم ارائه اطلاعات احراز هویت یا اطلاعات نامعتبر.

3. 403 Forbidden:
   - توضیح :این کد نشان‌دهنده این است که کلاینت مجوز دسترسی به منبع درخواست شده را ندارد.
   - علت وقوع :محدودیت‌های دسترسی، ممنوعیت دسترسی به منبع.
4. 404 Not Found:
   - توضیح :این کد نشان‌دهنده این است که منبع درخواست شده یافت نشده است.
   - علت وقوع URL :نامعتبر، حذف شدن منبع.

کدهای 5x (خطاهای سرور):

این کدها نشان‌دهنده این هستند که خطایی در سمت سرور رخ داده است و سرور نمی‌تواند درخواست معتبر کلاینت را پردازش کند.

1. 500 Internal Server Error:
   - توضیح :این کد نشان‌دهنده این است که سرور با یک شرایط غیرمنتظره مواجه شده است که مانع از انجام درخواست می‌شود.
   - علت وقوع :خطاهای داخلی سرور، مشکلات در کد سرور.
2. 502 Bad Gateway:
   - توضیح :این کد نشان‌دهنده این است که سرور به عنوان یک گیتوی یا پروکسی، پاسخ نامعتبری از سرور بالادستی دریافت کرده است.
   - علت وقوع :مشکلات در ارتباط بین سرورها، سرور بالادستی در دسترس نیست.
3. 503 Service Unavailable:
   - توضیح :این کد نشان‌دهنده این است که سرور موقتاً قادر به پردازش درخواست نیست، معمولاً به دلیل overload یا تعمیرات.
   - علت وقوع :ترافیک زیاد، تعمیرات سرور.
4. 504 Gateway Timeout:
   - توضیح :این کد نشان‌دهنده این است که سرور به عنوان یک گیتوی یا پروکسی، در زمان مشخص شده پاسخی از سرور بالادستی دریافت نکرده است.
   - علت وقوع :زمان‌بندی پاسخ سرور بالادستی، مشکلات شبکه.

سوال 4: سه نمونه از حملات که از طریق Payload انجام میشود را توضیح دهید؛ مثلا Sql injection.

جواب:

۱- Command Injection (تزریق دستور):

- توضیح :در این حمله، مهاجم یک دستور مخرب را در Payload ارسال می‌کند تا آن را در سیستم عامل سرور اجرا کند. این حمله معمولاً زمانی اتفاق می‌افتد که ورودی کاربر به درستی اعتبارسنجی نشده باشد.

```
; ls -la; echo "Hacked"
```

  - این Payload دستور ls -la را اجرا می‌کند تا لیست فایل‌ها و دایرکتوری‌ها را نمایش دهد و سپس پیام "Hacked" را چاپ می‌کند.
- اثرات : اجرای دستورات دلخواه روی سرور، سرقت اطلاعات، حذف یا تغییر فایل‌ها.

۲- SQL Injection (تزریق SQL):

- توضیح :در این حمله، مهاجم یک Payloadحاوی دستورات SQL مخرب را به پایگاه داده ارسال می‌کند تا دسترسی غیرمجاز به داده‌ها یا تغییر آن‌ها را امکان‌پذیر کند.

```
' OR '1'='1
```

  - این Payload باعث می‌شود کوئری SQL همیشه true برگرداند و مهاجم بتواند به تمام داده‌های جدول دسترسی پیدا کند.

۳- Cross-Site Scripting (XSS) (اسکریپت‌نویسی بین سایت‌ها):

- توضیح :در این حمله، مهاجم یک Payload حاوی کدهای JavaScript مخرب را در یک وب‌سایت تزریق می‌کند. وقتی کاربران دیگر این صفحه را باز می‌کنند، کد مخرب در مرورگر آن‌ها اجرا می‌شود.

```
<script>alert('XSS Attack!');</script>
```

  - این Payload یک پیام هشدار (alert) در مرورگر کاربر نمایش می‌دهد.
- علت وقوع :عدم اعتبارسنجی و escape کردن ورودی‌های کاربر در وب‌سایت.
- اثرات این نوع حمله سرقت کوکی‌ها، جعل هویت، تغییر محتوای صفحه، ریدایرکت کاربران به سایت‌های مخرب.

سوال 5: استخراج داده های حساس از HTTP.

جواب:

دستور زیر را در CMD اجرا میکنیم تا یک درخواست POST با نام کاربری و رمز عبور ارسال شود:

```
curl -X POST http://example.com/login -d "username=Hossein Tatar&password=40133014"
```

حال در Wireshark، از فیلتر زیر استفاده میکنیم تا فقط درخواست‌های POST را مشاهده کنیم:

```
http.request.method == "POST"
```

سپس می‌توانیم جزئیات درخواست را بررسی کرده و نام کاربری و رمز عبور را در بخش Form Data مشاهده کنیم مانند تصویر زیر: