

## ۳ - آشنایی با نرم افزار Wireshark

### ۳-۱ - هدف آزمایش

در این آزمایش با نرم افزار Wireshark آشنا می شویم تا بتوانیم با کمک این ابزار، ترافیک شبکه را ضبط، تحلیل و پروتکل های مختلف را در لایه های گوناگون شناسایی کنیم.

### ۳-۲ - قطعات و ابزارهای مورد نیاز

- نرم افزار Wireshark نسخه ۲ به بعد
- سیستم عامل ویندوز ۷ به بعد
- دسترسی به اینترنت

### ۳-۳ - مطالب مقدماتی

نرم افزار Wireshark یک تحلیلگر بسته های شبکه است که امکان مشاهده و بررسی ترافیک شبکه در سیستم عامل های ویندوز و لینوکس را به کاربران می دهد. این نرم افزار در سال ۱۹۹۸ با نام Ethereal توسط Gerald Combs آغاز شد و در سال ۲۰۰۶ به Wireshark تغییر نام داد. این ابزار با استفاده از چارچوب Qt و به زبان های C/C++ توسعه یافته و قادر به تحلیل آنلاین بیش از ۱۰۰۰ پروتکل در نسخه های مختلف خود می باشد. همچنین این برنامه می تواند اطلاعات خروجی از ابزارهایی مانند، TCPdump و Microsoft Network Monitor را خوانده و در فرمت های CSV، XML، PostScript یا Plaintext ذخیره کند.

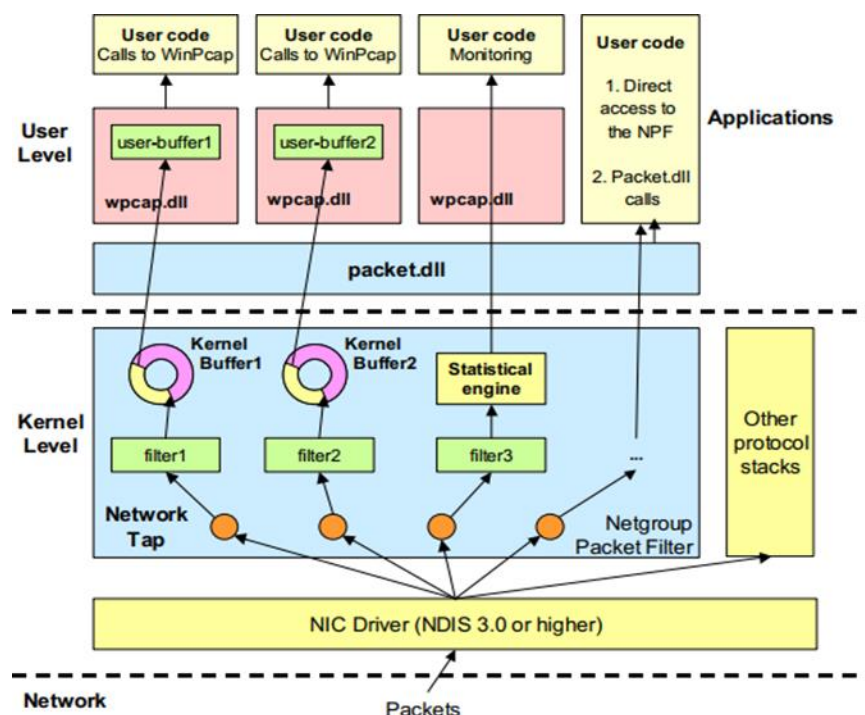
اسنیفر (Sniffer) ابزاری است که ترافیک شبکه را به صورت زنده دریافت و تحلیل می کند. به کمک اسنیفر، می توان بسته های ارسالی و دریافتی در شبکه را ضبط کرده و جزئیات پروتکل ها و داده ها را بررسی نمود. نرم افزار Wireshark به عنوان یک اسنیفر پیشرفته، امکان بررسی دقیق و تحلیل عمیق ترافیک شبکه را فراهم می آورد.

در سیستم عامل ویندوز، Wireshark از کتابخانه دریافت بسته (WinPcap) برای کار با ترافیک شبکه استفاده می کند. معماری WinPcap شامل دو بخش اصلی است (در تصویر ۱-۱ معماری کلی آن را مشاهده می کنید):

- بافرهای کرنل و کاربر: برای ذخیره و مدیریت داده های دریافت شده از شبکه.
- ماشین فیلترکننده: که فیلترهایی را به بسته های دریافتی اعمال می کند. همچنین، فایل های wpcap.dll و packet.dll به عنوان رابط های نرم افزاری بین Wireshark و WinPcap عمل می کنند تا دسترسی به بسته های شبکه فراهم شود.

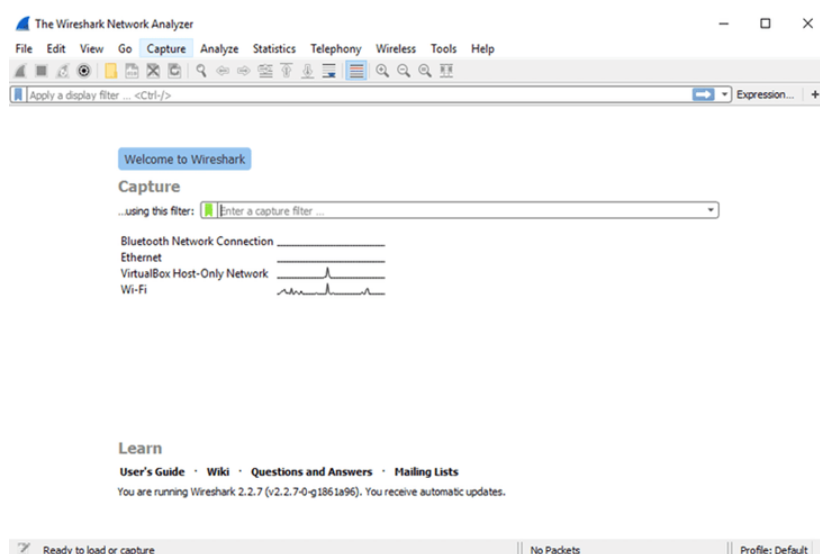
کاربر می تواند با استفاده از ابزارهای فیلترینگ ارائه شده توسط WinPcap، بسته های مورد نظر را از میان ترافیک کلی شبکه انتخاب کند. به عنوان مثال، با تعریف یک فیلتر از طریق Packet Netgroup Filter (NPF)، می توان بسته های مربوط به پروتکل UDP یا سایر پروتکل ها را انتخاب و دریافت نمود WinPcap. به صورت خودکار یک کپی از بسته های دریافت شده تهیه می کند

و این بسته‌ها پس از پردازش، به سایر لایه‌های پروتکل‌های موجود در سیستم عامل نیز ارسال می‌شوند. این فرآیند تضمین می‌کند که تحلیل ترافیک شبکه با دقت و کارایی بالایی انجام شود.



تصویر ۱-۱) معماری نرم‌افزار wireshark

برای شروع ابتدا واسط شبکه‌ای که قصد بررسی بسته‌های آن را داریم، مشخص می‌کنیم. همان‌طور که در تصویر زیر (۱-۲) مشاهده می‌کنید چهار واسط وجود دارد که بسته به سیستم شما ممکن است تعداد آن‌ها متفاوت باشد (توجه داشته باشید که واسط شبکه انتخابی شما باید به اینترنت متصل باشد).



تصویر ۱-۲) صفحه اولیه و انتخاب واسط شبکه در نرم‌افزار wireshark

حال پس از انتخاب واسط شبکه عملیات شنود و دریافت بسته‌ها را آغاز کنید و پس از مدتی عملیات را متوقف کنید (مانند تصویر ۳-۱) همچنین می‌توانید با دکمه‌های ترکیبی CTRL+E عملیات شنود را آغاز و متوقف کنید.



تصویر ۳-۱) عملیات آغاز دریافت بسته‌ها از واسط شبکه مشخص شده

در ادامه برنامه شروع بده دریافت بسته‌ها از واسط انتخابی می‌کند. معمولاً هر سطر یک بسته را نشان می‌دهد. همان‌گونه که مشاهده می‌کنید بسته‌ها با رنگ‌های مختلف نمایش داده شده‌اند. قوانین رنگ گذاری Wireshark از بخش:

View -> Coloring rules قابل دسترس است. همان‌طور که در تصویر زیر مشاهده می‌کنید (تصویر ۳-۲)، هر بسته در هر سطر به همراه توضیحاتی مانند نوع پروتکل، آدرس مبدا و زمان دریافت بسته مشخص شده است همچنین توضیحات بیشتری را در مورد بسته می‌توانید در زیر مشاهده کنید.

No.	Time	Source	Destination	Protocol	Length	Info
319	13.155301	172.24.72.86	172.24.72.11	HTTP	251	GET /iFADevice.xml HTTP/1.1
320	13.155969	172.24.72.15	172.24.72.86	TCP	62	1990 → 16600 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
321	13.156037	172.24.72.86	172.24.72.15	TCP	54	16600 → 1990 [ACK] Seq=1 Ack=1 Win=64240 Len=0
322	13.156276	172.24.72.86	172.24.72.15	HTTP	251	GET /iFADevice.xml HTTP/1.1
323	13.156966	172.24.72.17	172.24.72.86	TCP	60	1990 → 16597 [ACK] Seq=1 Ack=198 Win=6432 Len=0
324	13.157388	172.24.72.86	172.24.72.248	TCP	62	16602 → 50142 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
325	13.157966	172.24.72.17	172.24.72.86	TCP	156	1990 → 16597 [PSH, ACK] Seq=1 Ack=198 Win=6432 Len=102 [TCP segment of a reassembled PDU]
326	13.159402	172.24.72.86	172.24.72.18	TCP	62	16603 → 49152 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
327	13.160375	172.24.72.86	172.24.72.16	TCP	62	16604 → 1990 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
328	13.167289	172.24.72.86	172.24.72.13	TCP	62	16605 → 1990 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
329	13.172960	172.24.72.17	172.24.72.86	HTTP/XML	1054	HTTP/1.1 200 OK
330	13.173048	172.24.72.86	172.24.72.17	TCP	54	16597 → 1990 [ACK] Seq=198 Ack=1104 Win=63138 Len=0

Frame 326: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0	سرآیند پروتکل‌ها در لایه‌های مختلف یک بسته (در صورت وجود، به همراه داده لایه کاربرد)
Ethernet II, Src: Tp-Link_T11:1b:f6 (90:f6:92:11:1b:f6), Dst: BelkinIn_63:a8:2c (b4:75:0e:63:a8:2c)	
Internet Protocol Version 4, Src: 172.24.72.86, Dst: 172.24.72.18	
Transmission Control Protocol, Src Port: 16603, Dst Port: 49152, Seq: 0, Len: 0	

0000 04 75 0e 63 a8 2c 90 f6 52 11 1b f6 00 00 45 00	نمایش یک بسته Hex
0010 00 10 51 1e 40 00 00 00 c1 10 ac 18 40 50 ac 18	
0020 42 12 40 d0 c0 00 00 00 00 1f 00 00 00 70 00	
0030 20 00 c4 23 00 00 00 00 05 04 01 01 04 00	

تصویر ۳-۲) بسته‌های دریافت شده توسط نرم‌افزار و توضیحات مرتبط با هر بسته

### ۳-۴- شرح آزمایش

\*در تمام بخش‌های آزمایش، واسطی که با آن دسترسی به اینترنت دارید را برای شنود بسته انتخاب کنید.

### ۱-۴-۳- لایه‌بندی پروتکل‌ها

شروع به شنود بسته‌ها کنید. به اینترنت وارد شوید، شروع به وب گردی کنید و پس از گذشت سه دقیقه شنود را متوقف کنید.

سوال ۱: به یک بخش دلخواه از بسته‌های شنود شده مراجعه کنید. چه پروتکل‌هایی را مشاهده می‌کنید. لیست آنها را یادداشت کنید.

سوال ۲: یک بسته را به دلخواه انتخاب کنید. مشخص کنید که چه پروتکل‌هایی در لایه‌های مختلف آن استفاده شده است. ترتیب قرارگیری بیت‌ها داخل بسته چه ارتباطی با لایه‌های مختلف دارد؟ اندازه فریم لایه دو این بسته چقدر است؟ اندازه بسته لایه ۳ چقدر است؟

سوال ۳: آیا می‌توانید بسته‌هایی را پیدا کنید که بدون پروتکل‌های لایه‌های Network، Transport و Application باشند؟

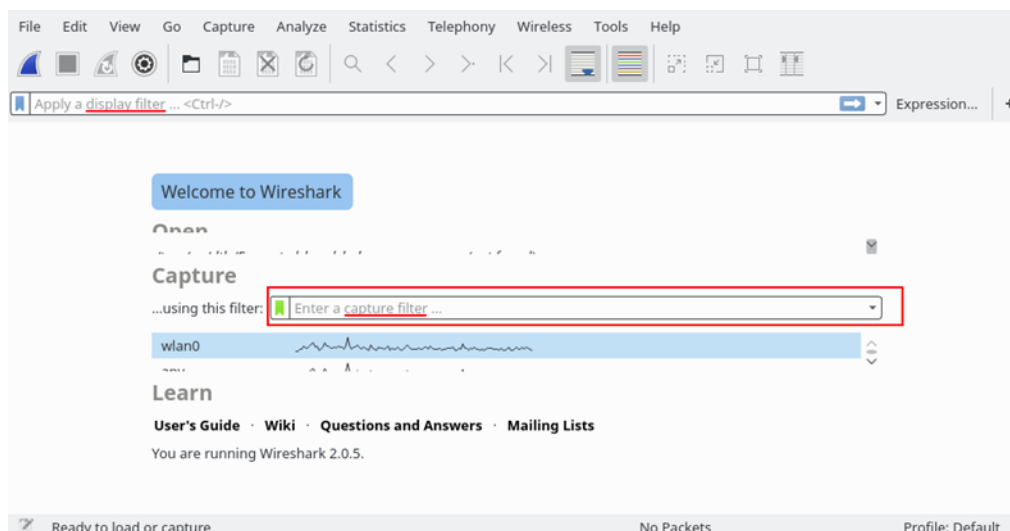
سوال ۴: این بسته‌ها از چه پروتکلی استفاده کرده‌اند؟

سوال ۵: از یکی از بسته‌ها بخش مربوط به پروتکل Protocol(IP) Internet را پیدا کنید. Checksum. پروتکل IP را پیدا کنید و آن را یادداشت کنید.

سوال ۶: از یکی از بسته‌ها بخش مربوط به پروتکل Protocol(TCP) Control Transport و یا Protocol(UDP) Datagram User را پیدا کنید. عدد مربوط به Port مبدا و مقصد را یادداشت کنید. به نظر شما این اعداد در مبدا و مقصد چه چیزی را مشخص می‌کند؟ Checksum مربوط به پروتکل‌های TCP و UDP را مشخص کنید.

### ۲-۴-۳- کار با فیلترکننده بسته‌ها

برنامه Wireshark دو نوع فیلتر کننده بسته دارد. یک نوع Filter Capture است و نوع دیگر Filter Display. Filter Capture قبل از شروع به شنود بسته مقداردهی می‌شود و در حقیقت همان فیلتری است که توسط NPF بر روی بسته‌های دریافت شده از گرداننده شبکه اعمال می‌گردد. بنابراین این فیلتر بر جمع‌آوری بسته‌ها تاثیر می‌گذارد. در مقابل Filter Display صرفاً مربوط به فیلتر کردن بسته‌های جمع‌آوری شده است. با استفاده از Filter Display می‌توان تعدادی از بسته‌های جمع‌آوری شده را مشخص کرد که در پنجره Wireshark نمایش داده شوند. این تفاوت در تصویر ۱-۵ نیز نمایش داده شده است.



تصویر ۱-۵) انواع فیلتر بسته‌ها

### ۱-۲-۳-۴- کار با capture filter

۱. به صفحه اول برنامه بروید و در قسمت Filter Capture ، مقدار port 53 را وارد کنید .
۲. حال واسط شبکه موردنظر خود را انتخاب کنید.
۳. در command prompt دستور ping google.com را وارد کنید.
۴. سپس دستور nslookup 1.1.1.1 را وارد کنید.
۵. حال شنود بسته‌ها را متوقف کرده و شما باید صرفا پروتکل‌های DNS را در wireshark مشاهده کنید .

سوال ۷: یکی از بسته‌ها که از سیستم شما ارسال شده است را انتخاب کنید. پروتکل لایه Transport چیست؟ آدرس IP مقصد چیست؟ سرایند لایه دوم را انتخاب کنید. آدرس مبدا و مقصد را یادداشت کنید.

سوال ۸: کدامیک از آدرس‌های پیدا کرده در بخش قبل را می‌توانید در خروجی دستور all ipconfig/مشاهده کنید؟

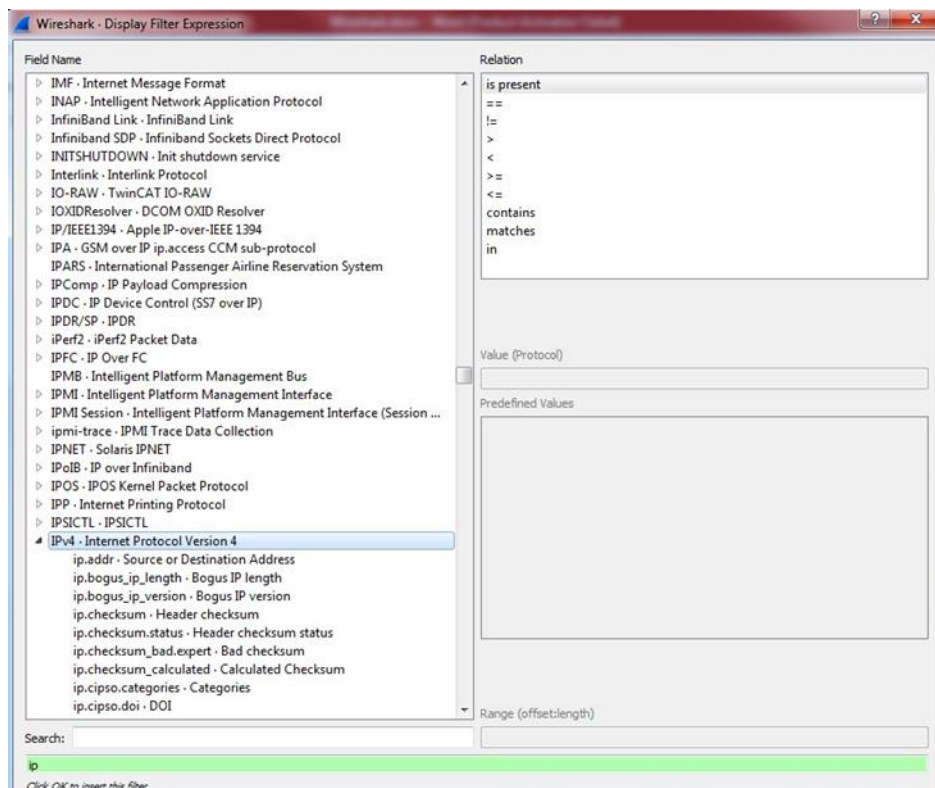
سوال ۹: یک بسته مربوط به دستور Ping را انتخاب کنید و به بخش مربوط به پروتکل DNS در آن بروید. به بخش Queries بروید. چه type ای انتخاب شده است؟ به نظر شما این درخواست DNS برای چه کاری استفاده شده است؟

سوال ۱۰: یک بسته مربوط به دستور nslookup را انتخاب کنید و به بخش مربوط به پروتکل DNS در آن بروید. به بخش Queries بروید. چه type ای انتخاب شده است؟ بده نظر شما این درخواست DNS برای چه کاری استفاده شده است؟

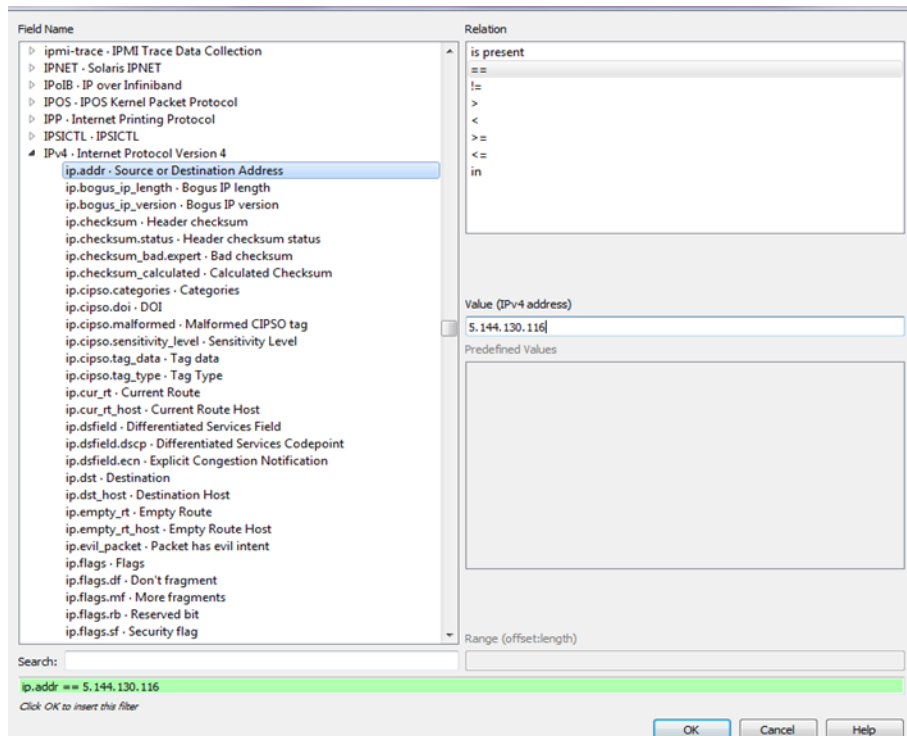
سوال ۱۱: به نظر شما چه type های دیگری ممکن است وجود داشته باشد؟ سه مورد را یادداشت کنید.

## ۲-۲-۴-۳ کار با display filter

۱. دوباره به صفحه اول برنامه بروید. این بار واسط شبکه را بدون هیچ Filter Capture ای انتخاب کنید.
۲. در command prompt دستور `tracert p30download.com` را وارد کنید. منتظر بمانید تا کار دستور به اتمام برسد.
۳. بدون اینکه شنود بسته را متوقف کنید در قسمت `filter display` مقدار `dns` را تایپ کنید و اینتر را بزنید. مشاهده میکنید که صرفا بسته‌های مربوط به پروتکل DNS انتخاب شدند در حالی که سایر بسته‌ها نیز در حال دریافت شدن از گرداننده کارت شبکه هستند.
۴. در قسمت `display filter` ، کلیک راست کنید و بر روی `display filter expression` کلیک کنید. مانند تصویر ۶-۱ صفحه‌ای باز شده و واژه `ip` را جستجو کنید و مقدار `ipv4` را انتخاب کنید .
۵. از زیر بخشهای `IPv4` ، بخش `ip.addr` را انتخاب کنید. سپس از بخش `relation` ، مقدار `==` را انتخاب کرده و در بخش `Value` آدرس IP که از دستور `tracert` به شما گزارش شده است را وارد کنید. به عنوان مثال برای آدرس `p30download.com` به تصویر ۷-۱ مراجعه کنید .



تصویر ۶-۱ انتخاب display filter



تصویر ۱-۷) مقادیر برای p30download.com

سوال ۱۲: بعد از کلیک کردن بر روی OK چه اتفاقی میافتد؟ در بسته‌هایی که مشخص شده‌اند چه پروتکل‌هایی را مشاهده می‌کنید؟

سوال ۱۳: اولین بسته را انتخاب کنید. به بخش پروتکل Internet Control Message Protocol بروید. مقدار type را مشخص کنید. به بخش مربوط به پروتکل IP بروید و مقدار TTL را یادداشت کنید.

۶. برای بسته‌هایی که مبدا آنها ماشین شماسست مقدار TTL را یادداشت کنید. این مقدار در حدال تغییر است.

سوال ۱۴: به نظر شما هدف از تغییر این مقدار چیست؟ می‌توانید با مراجعه به هدف دستور tracert آن را شرح دهید.

۷. از بخش فیلتر، مقدار فیلتر را به دستور ip.proto == تغییر دهید .

سوال ۱۵: این فیلتر چه کاری انجام می‌دهد؟