به نام خدا

آزمایشگاه شبکه و امنیت

تجزیه و تحلیل بسته ها

آشنایی با نرم‌افزار Wireshark

با بررسی پروتکل های لایه کاربرد(HTTP,DNS)

دکتر علی فانیان، مهندس تهمینه شبانیان

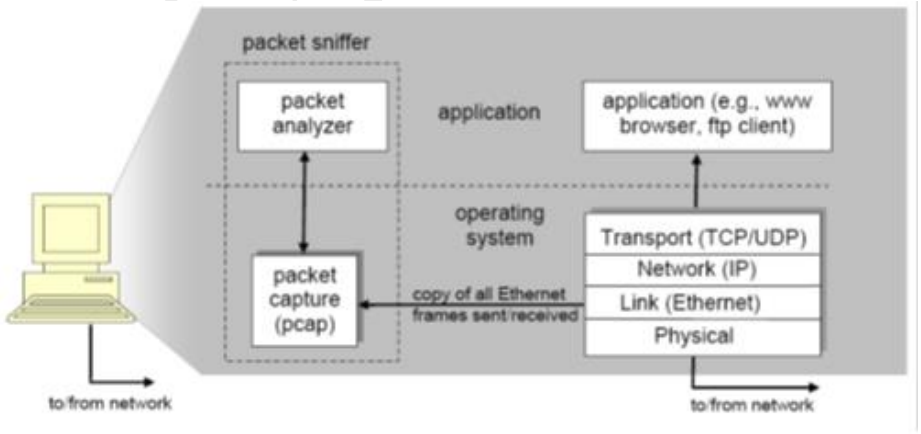
۱- مقدمه

درک پروتکل های شبکه تا حد زیادی به دیدن عملکرد وکار با آنها بستگی دارد. مشاهده دنباله ای ازپیام های رد و بدل شده بین دونهاد پروتکل[1]، دقت به جزییات مربوط به عملیات پروتکل، مجبور نمودن پروتکل به انجام عملیات خاص ومشاهده این اقدامات وعواقب آن در شبکه می تواند به درک بهتر پروتکل ها کمک نماید. این فعالیت ها را می توان در شبیه سازها یا در یک شبکه واقعی مثل اینترنت انجام داد.

در شبکه اینترنت برای مشاهده پیام های مبادله شده بین نهادهای اجرایی پروتکل، ازpacket snifferها استفاده می‌شود. همانطور که از نامشان پیداست packet snifferها پیام هایی را که توسط کامپیوتر شما ارسال یا دریافت می شوند را گرفته و معمولا محتویات موجود در پروتکل های مختلف را نمایش داده یا ذخیره می‌نمایند.

packet sniffer یک نرم افزارغیر فعال[2] است یعنی پیام های مبادله شده و همچنین پروتکل های در حال اجرا بر روی کامپیوتر شما را مشاهده می کند ولی خودش هرگز بسته ای نمی فرستد و به طور مشابه، هرگز بسته ی دریافتی، مستقیما به packet sniffer آدرس دهی نمی شوند.

به طور کلی ساختار یک packet sniffer به صورت زیر است. در این ساختار، نسخه ای از فریم های رد و بدل شده از کارت شبکه توسط کتابخانه pcap دریافت می گردد. آنگاه محتوای فیلد های مختلف پروتکل های مربوط به پیام های رد و بدلی توسط نرم‌افزار آنالیز کننده بسته‌ها در لایه های مختلف نشان داده می شود. بدین منظور بایستی این نرم افزار از رفتار و نحوه عملکرد و ساختار پروتکل های مورد نظر آگاهی داشته باشد.



[1] protocol entities
[2] passive

packet Sniffer ها انواع مختلف دارند مثل:

EtherDetect Packet Sniffer، MSN Sniffer ،Smart Sniffer،IP sniffer, wireshark و...

- در این آزمایشگاه از Wireshark packet sniffer استفاده می شود، این نرم افزار امکان مشاهده محتوای پیام‌های ارسالی و دریافتی از طریق پروتکل های موجود در سطوح مختلف پشته ی پروتکل[3] را فراهم می‌نماید.

۲- آشنایی با wireshark

اولین بارآقایGerald Combs شروع‌به نوشتن برنامه‌ای با نام Etherealکرد که بار نخست در سال ۱۹۹۸ عرضه شد و تاکنون بیشتر از ۵۰۰ نسخه از آن توسط نویسندگان مختلف عرضه شده است. این ابزار با نام اولیهEthereal عرضه شد، اما در مه ۲۰۰۶ پروژه به نام Wireshark تغییر نام یافت. در حقیقت قدرت این ابزار به دلیل وجود سه خصوصیت زیر می‌باشد:

- سادگی نصب
- سادگی استفاده از رابط گرافیکی
- قابلیت انجام عملیات های متنوع بر روی بسته های جمع آوری شده

Wireshark یک ابزار مفید و رایگان برای شنود و تحلیل ترافیک شبکه در سیستم های ویندوزی و لینوکسی است که، صدها پروتکل را شناخته و پشتیبانی می کند. این ابزار توانایی بررسی داده ها به صورت زنده یا از روی فایل ذخیره شده را دارد. Wireshark امکانات مختلفی از قبیل فیلترنمودن، نمایش اطلاعات و نظارت بر ترافیک عبوری شبکه را در اختیار استفاده‌کنندگان قرار می‌دهد. همچنین این ابزار برای رفع مشکلات شبکه، بررسی و توسعه نرم افزارها و پروتکل های ارتباطی استفاده می شود و می توان آنرا یکی از محبوب‌ترین ابزارها در زمینه بررسی شبکه به شمار آورد.

مستندات و فایل های آموزشی زیادی در مورد نرم افزار Wireshark در وبسایت این نرم افزار موجود است:

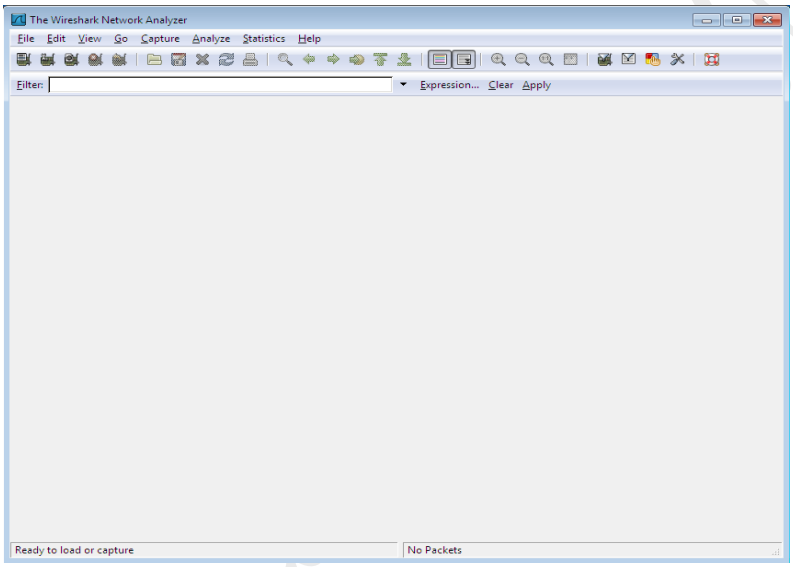
- راهنمای کاربر http://www.wireshark.org/docs/wsug_html_chunked/
- دستور کار http://www.wireshark.org/docs/man-pages/
- بخش پرسش و پاسخ جام http://www.wireshark.org/faq.html

[3] protocol stack

۲-۱ راه اندازی Wireshark

برای نصب برنامه wireshark باید کتابخانه libpcap برای دریافت ترافیک شبکه روی سیستم نصب بوده و در غیر این صورت با نصب wireshrak برنامه های لازم به صورت اتوماتیک نصب خواهند شد. این نرم افزار را میتوان از آدرس http://www.wireshark.org/download.html دانلود کرد.

زمانی که برنامه Wireshark اجرا شود پنجره ای مانند شکل ۱ نمایش داده می شود.



شکل ۱

۲-۲ معرفی رابط گرافیکی نرم افزار

این رابط از پنج بخش اصلی (شکل ۲) تشکیل شده است که به معرفی آن ها خواهیم پرداخت:

- **command menus:**

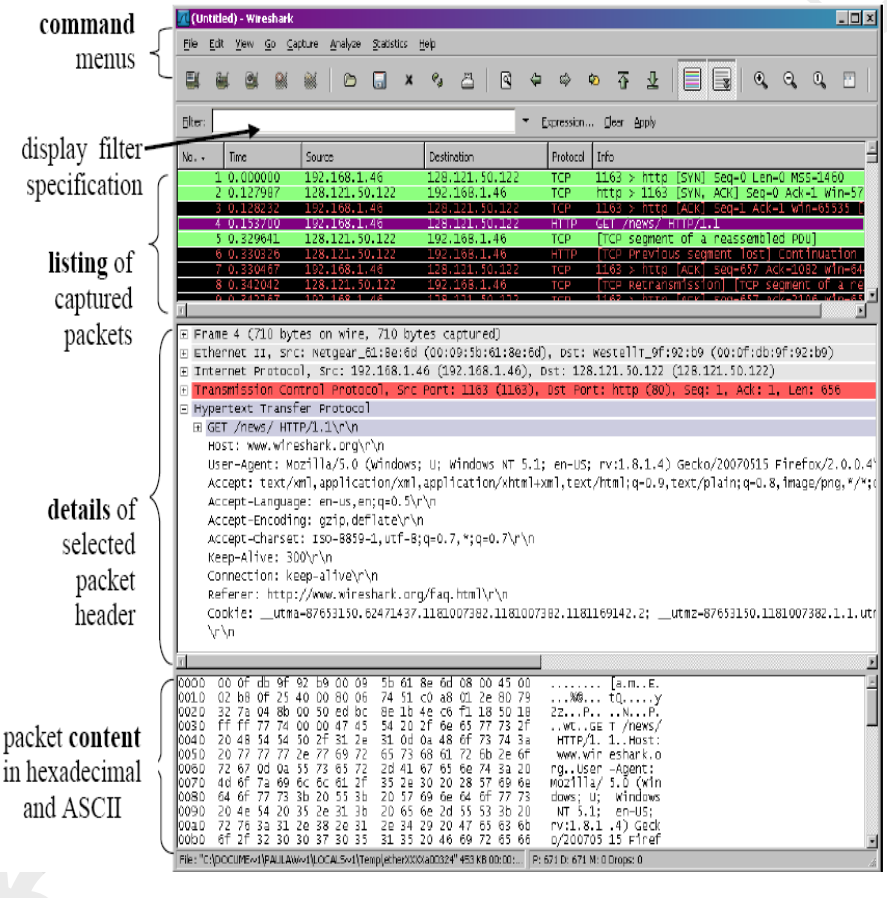
این منوها به صورت استاندارد در بالای پنجره قرار دارند. از بین این منوها، دو منوی File و Capture کاربرد بیشتری دارند. منوی فایل امکان ذخیره و باز کردن بسته های جمع آوری شده[۴] و خروج از نرم افزار را فراهم می نماید و منوی Capture امکان شروع جمع آوری بسته ها را.

- **packet-listing window:**

این پنجره خلاصه ای یک خطی از هر بسته جمع آوری شده را، نشان می دهد. این خلاصه شامل شماره بسته، زمان دریافت آن، آدرس منبع و مقصد، نوع پروتکل و اطلاعات خاص پروتکل موجود در بسته است. به این

[4] Capture

نکته توجه داشته باشید که، شماره بسته، نشان دهنده ترتیب دریافت بسته ها توسط Wireshark بوده و ارتباطی با شماره بسته درسرآیند[5] پروتکل ندارد. این پنجره می تواند اطلاعات را براساس هر کدام از دسته بندی ها با کلیک بر روی نام ستون مرتب نماید. در فیلد پروتکل بالاترین سطح پروتکلی که بسته را می فرستد یا دریافت می کند، نمایش داده می شود. به عبارت دیگر پروتکلی که توسط منبع یا مقصد[6] نهایی بسته مورد استفاده قرار گرفته است.

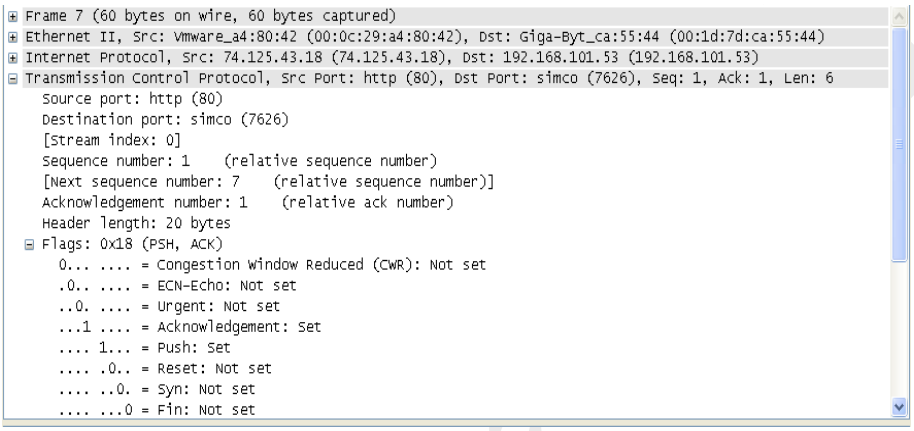


شکل ۲: Wireshark Graphical User Interface

[5] header
[6] sink

- **packet-header details window:**

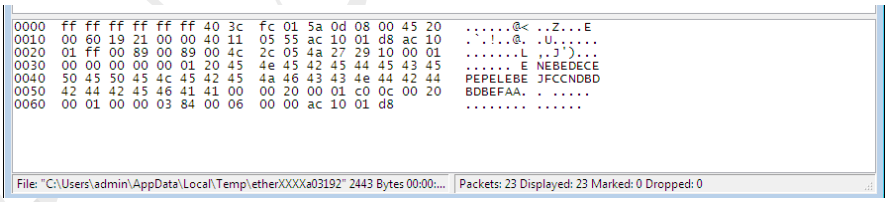
این پنجره جزییات بیشتری را درباره بسته انتخاب شده در packet-listing window نشان می دهد. اینجزییات شامل اطلاعاتی مربوط به فریم اترنت ودیتا گرام IP است. با کلیک بر روی علامت + در سمت چپ فریم، اترنت یا دیتاگرام IP می توان اطلاعات بیشتری کسب نمود. اگر بسته از طریق TCP یا UDP منتقل شود، جزییات مربوط به آنها نیز نمایش داده خواهد شد.



شکل۲: packet-listing window

- **packet-contents window:**

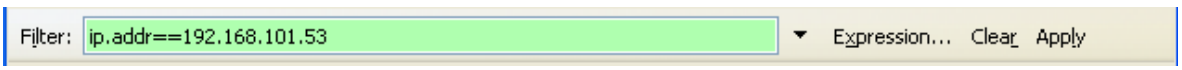
این پنجره تمام محتویات بسته های جمع آوری شده را به هر دو فرمت اسکی (ASCII) و هگزادسیمال نشان می‌دهد.(شکل ۳)



شکل ۳

- **filter field:**

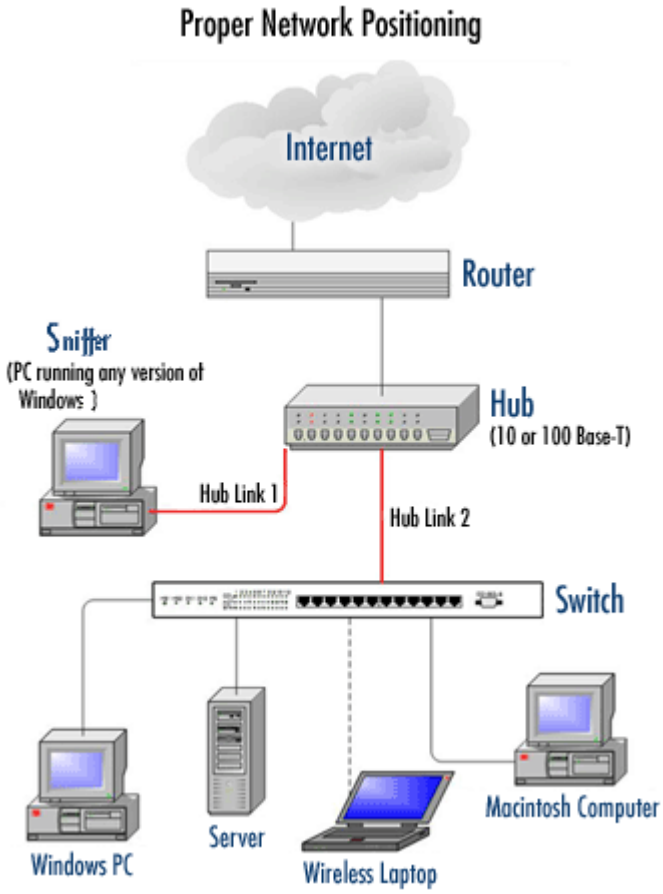
در بالای صفحه نمایش فیلد fillter وجود دارد، که برای فیلتر کردن اطلاعات packet-listing window استفاده می شود. برای این کار می توان نام پروتکل یا اطلاعات دیگر رادر این فیلد وارد نمود.



شکل ۴: filter fileld

دنیای شبکه

Wireshark همچنین به عنوان ابزاری قدرتمند به منظور بررسی وضعیت شبکه محسوب می شود. از طریق این نرم افزار می توان الگوی ترافیکی شبکه را بررسی نمود و به عیب یابی در شبکه پرداخت. در شکل زیر ترافیک خروجی شبکه یعنی ترافیکی که به دروازه شبکه منتقل می شود توسط یک نرم افزار packet sniffer در حال شنود است. این ترافیک می تواند توسط مدیر شبکه بررسی و تحلیل گردد. (یادآوری می‌شود استفاده از Hub در نقاط حساس شبکه که امکان شنود اطلاعات توسط افراد دیگر وجود دارد توصیه نمی شود.)



از سوی دیگر wireshark می تواند توسط افراد مزاحم نیز مورد استفاده قرار گیرد.

- ☐ شنود اطلاعات clear text
- ☐ جمع آوری اطلاعات از پروتکل های آسیب پذیری مانند HTTP, FTP, POP3, IMAP, SMATP,…
- ☐ شنود داده های VOIP
- ☐ کشف الگوی ترافیک شبکه

دنیای شبکه

۱. چند نمونه نرم افزار مانیتورینگ شبکه نام ببرید. مقایسه ای بین مشخصات، ابزارها و امکانات این نرم افزارها انجام دهید.

به نام خدا

آزمایشگاه شبکه و امنیت

تجزیه و تحلیل بسته ها

آشنایی با پروتکل‌های لایه کاربرد

HTTP, DNS

دکتر علی فانیان، مهندس تهمینه شبانیان

۱- پروتکل HTTP

پیش از ورود به بحث پروتکل HTTP نگاهی به برخی مفاهیم وب می پردازیم.

وب چیست؟

World Wide Web (WWW) که معمولابه عنوان Web شناخته می شود،

- شبکه‌ای از کامپیوترها در سراسر دنیا است.
- همه کامپیوترها در سراسر دنیا می‌توانند از طریق وب با یکدیگر ارتباط برقرار کنند.
- **پروتکل ارتباطی برای ارتباطات وب HTTP نام دارد.**
- اطلاعات درون فایل هایی که صفحه وب نامیده می شوند، ذخیره می گردند.
- صفحات وب بر روی web server ها ذخیره می گردند.
- کامپیوترهایی که صفحات وب را می خوانند web client خوانده می شوند.
- Web client ها صفحات وب را از طریق نرم افزارهای مرورگرمشاهده می نمایند.
- معروفترین نرم افزار های مرورگر عبارتند از Internet Explorer, FireFox, Chrom ,....
- استانداردهای وب توسط کنسرسیوم (World Wide Web Consortiums) W3C تعیین می گردد.
- صفحات وب بر اساس زبان نشانه گذاری HTML نمایش داده می شوند.

HTML چیست؟

Hyper Text Murkup Language(HTML) یک زبان نشانه گذاری جهانی برای وب است. HTML به شما اجازه خواهد داد که متن را قالب بندی کنید، گرافیک اضافه کنید، لینک ها، فرم های ورودی، قالب ها و جدول ها را ایجاد کنید و همه آن ها را در یک فایل متنی که مرورگرها می توانند بخوانند و نمایش دهند، ذخیره کنید. کلید HTML تگ ها هستند که نشان می دهند چه محتوایی بالا آمده است. فرم کلی فایل های HTML به صورت زیر است.

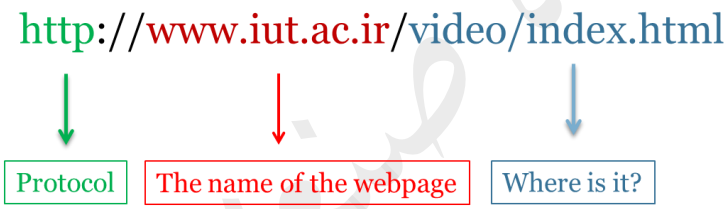
```
<html>
<body>

  <h1>My First Heading</h1>

  <p>My first paragraph.</p>

</body>
</html>
```

? سوال ۱ : **به وب سایت www.w3schools.com مراجعه کنید و در مورد نحوه عملکرد HTML5 توضیح دهید.**

URI چیست؟

URI (Uniform Resource Identifier)، یک رشته از کاراکترهاست که یک محل یا آدرس از منابع را روی اینترنت نشان می دهد و تعیین می کند که چگونه باید به این منابع دسترسی پیدا کرد، URI در حقیقت مجموعه در برگیرنده URLمی باشد و از سه بخش اساسی تشکیل شده است:

- URC (Uniform Resource Classification)
- URL (Uniform Resource Locator)
- URN (Uniform Resource Name)



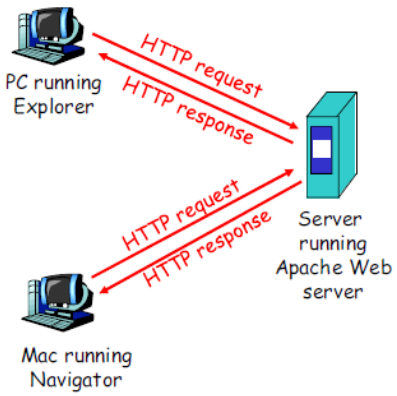
۱-۱-پروتکل HTTP چیست؟

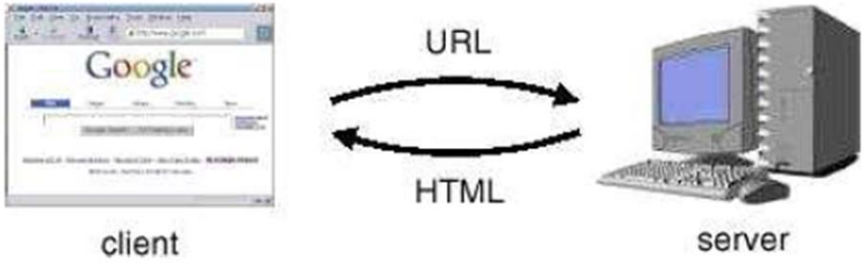
پروتکل(Hyper text transfer Protocol))HTTP مجموعه ای از قوانین برای انتقال فایل ها (متن، تصاویر گرافیکی، صدا، ویدئو و دیگر فایل های مولتی مدیا بین Web Serverها و Web Broswer ها است. وقتی کاربر مرورگر خود را باز می کند بطور غیر مستقیم استفاده از پروتکل HTTP را آغاز می نماید.

پایه پروتکل HTTP بر این مبنا است که، هر صفحه وب می تواند شامل یک لینک (Hyperlink) باشد، تا از این طریق بتوان به صفحات دیگر رفته و آنها را مشاهده نمود. HTTP یک پروتکل Client-Server بوده و از جفت‌های Request/Responseتشکیل شده است. در اینجا کلاینت همان User Agent (مرورگر شما) است و سرور یک وب سایت اینترنتی می باشد. هر گاه مرورگر درخواستی از وب سرور داشته باشد، درخواست خودش را از طریق قالب درخواست[۷](یک درخواست می‌تواند شامل ارسال اطلاعات login به یک سرور یا درخواست کد html یک صفحه

[7] Request

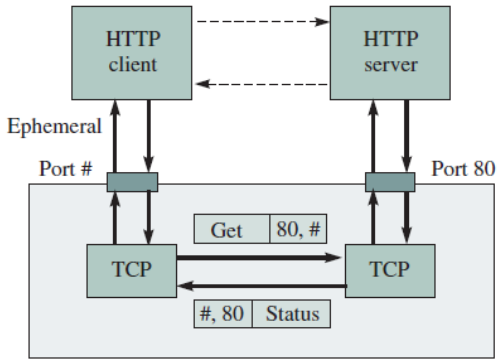
خاص باشد) به سرور می‌فرستد. سرور به ازای هر درخواست یک پاسخ[8] ارسال می نماید. داخل هر پاسخ اطلاعـاتی نظیـر جواب سرور، سرآیندها[9] و encoding قرار می گیرد.





HTTP در معماری شبکه در بالاترین لایه یعنی لایه Application قرار دارد. این پروتکل مبتنی بر text ساده اسـت و بـر پایه پروتکل انتقال TCP کار می‌نماید. دلیل اینکه HTTP از پروتکل TCP استفاده می کند و نه از UDP ایـن اسـت کـه، پروتکل TCP/IP درستی انتقال اطلاعات را برای گیرنده و فرستنده تضمین می نمایـد. پـورت پـیش فـرض بـرای پروتکـل HTTP، 80 است.

[8] Response
[9] header



۲-۱- مجموعه فرامین HTTP

نام فرمان	توضیح
GET	تقاضا برای دریافت یک صفحه وب از سرویس دهنده
HEAD	تقاضا برای دریافت سرآیند یک صفحه وب
PUT	تقاضا برای ذخیره کردن یک صفحه وب روی یک سرویس دهنده
POST	تقاضا برای ضمیمه کردن اطلاعاتی به یک منبع (مثل یک فایل یا صفحه)
DELETE	تقاضا برای حذف یک صفحه وب
LINK	تقاضای برقراری پیوند بین دو منبع موجود
UNLINK	تقاضای خاتمه پیوند دو منبع موجود

۳-۱-کدهای وضعیت[۱۰]

[10] statuse code

کد	عملکرد
1XX	اطلاع رسانی برای استفاده در آینده
2XX	انجام موفقیت آمیز تراکنش
3XX	راهنمائی مجدد
4XX	بروز خطاء سمت سرویس گیرنده
5XX	بروز خطاء سمت سرویس دهنده

کد وضعیت	عملکرد
200	تراکنش با موفقیت انجام شده است
201	دستور POST با موفقیت انجام شده است
202	درخواست ارسالی دریافت گردید.
300	منبع درخواستی در مکان های مختلفی پیدا شده است
301	منبع درخواستی به صورت دائم منتقل شده است
302	منبع درخواستی به صورت موقت منتقل شده است
400	درخواست نامناسب از جانب سرویس گیرنده
401	درخواست غیرمجاز
404	منبع درخواستی پیدا نگردید
500	بروز خطاء بر روی سرویس دهنده
501	متد استفاده شده ، پیاده سازی نشده است

نمونه ای از پیام درخواست کلاینت

```
GET /search?q=Introduction+to+XML+and+Web+Technologies HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7.2)
↳  Gecko/20040803
Accept: text/xml,application/xml,application/xhtml+xml,
↳  text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: da,en-us;q=0.8,en;q=0.5,sw;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.google.com/
```

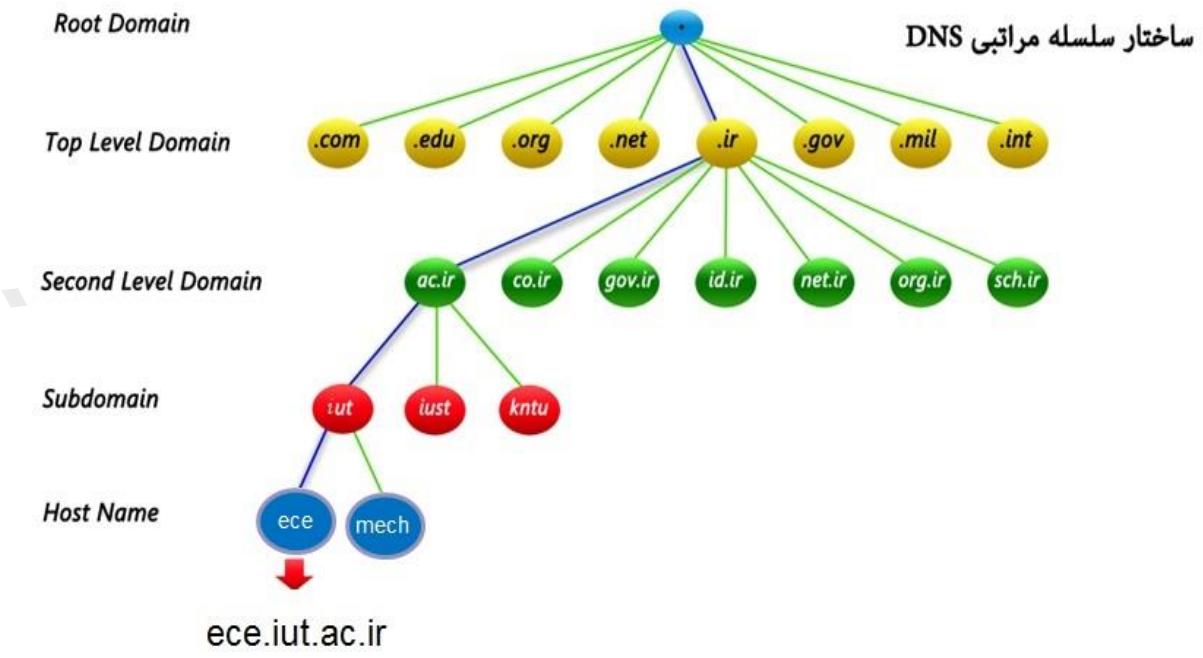
نمونه‌ای از پیام پاسخ سرور

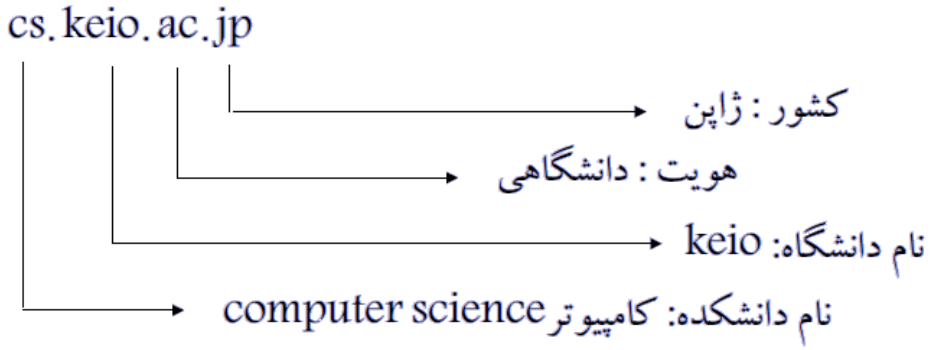
```
HTTP/1.1 200 OK
Date: Fri, 17 Sep 2009 07:59:01 GMT
Server: Apache/2.0.50 (Unix) mod_perl/1.99_10 Perl/v5.8.4
↳  mod_ssl/2.0.50 OpenSSL/0.9.7d DAV/2 PHP/4.3.8 mod_bigwig/2.1-3
Last-Modified: Tue, 24 Feb 2009 08:32:26 GMT
ETag: "ec002-afa-fd67ba80"
Accept-Ranges: bytes
Content-Length: 2810
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>...</html>
```

سوال ۲ : **پروتکل HTTPS چیست؟**

۲- پروتکل DNS

هر کامپیوتری که از شبکه اینترنت برای تبادل اطلاعات استفاده می کند یک Host یا میزبان نامیده می شود. در این شبکه هر میزبان توسط یک IP Address شناخته شده و از میزبان های دیگر متمایز می شود. این آدرس یک عدد ۳۲ بیتی مانند 87.248.112.181 بوده که به خاطر سپاری و استفاده از آن برای کاربران بسیار سخت می‌باشد. بنابراین برای سهولت کار می توان به هر میزبان یک عنوان مشخص کننده دیگر به نام Host Name اختصاص داد. این نام نیز مانند آدرس IP به صورت یکتا انتخاب می گردد و بصورت سلسله مراتبی می‌باشد. بگونه ای که مشهود است یک نام حوزه از چند بخش مجزا که با علامت "." از هم تفکیک شده اند، تشکیل می شود. بطور مثال www.yahoo.com. نام های حوزه شباهت ویژه ای به سیستم سلسله مراتبی ذخیره سازی فایل روی یک ماشین دارد. هر کدام از این بخش ها که "سطح" نام دارد به یک قسمت از بانک اطلاعاتی توزیع شده ای اشاره می نمایند، که به محدودتر شدن فضای جستجو کمک می کند. به‌عنوان مثال آدرس زیر بسادگی قابل تحلیل است:





تمامی اجزاء و پروتکل های شبکه تنها آدرس IP را شناخته و بر مبنای آن عمل می کنند، اما کاربران نهایی شبکه عموما تنها از آدرس URL میزبان مورد نظر خود اطلاع دارند. بنابراین یک برنامهٔ کاربردی پس از وارد شدن نام میزبان توسط کاربر، می بایست ابتدا آدرس IP میزبان مورد نظر را استخراج و سپس برای ارسال و دریافت اطلاعات اقدام نماید.

در شبکه برای بدست آوردن IP Address متناظر با نام میزبان، از کامپیوترهایی (میزبان یا سرور) با نام DNS Server کمک گرفته می شود. هر DNS Server حاوی یک پایگاه داده شامل نام میزبان و آدرس IP برخی میزبان های شبکه می باشد که با دریافت درخواست مبنی برتعیین آدرس IP یک میزبان، نام میزبان موجود در بسته با اطلاعات پایگاه داده سرور مقایسه شده و در صورت وجود، IP Address استخراج شده و به درخواست دهنده ارسال می گردند. برقراری ارتباط بین میزبان های شبکه و DNS سرور توسط پروتکل DNS انجام می شود. پروتکل DNS یک روش سلسله مراتبی است که بانک های اطلاعاتی مربوط به نام های نمادین و معادلIP آنها را روی کل شبکهٔ اینترنت توزیع کرده است. در DNS کل آدرس های اینترنت درون بانک های اطلاعاتی توزیع شده ای هستند که هیچ تمرکزی روی نقطه ای خاص از شبکه ندارند.

در ویندوز یک برنامه کاربردی قبل از هر کاری، ابتدا یک تابع کتابخانه ای[11] بـه نـام "تـابع تحلیلگـر نـام[12]" را فراخـوانی می‌کند. تابع تحلیلگر نام، آدرس نمادینی را که بایستی ترجمه شود، بعنوان پارامتر ورودی می پـذیرد و سـپس یـک بسـته درخواست[13] به روش UDP تولید می کند و به آدرس یک DNS سرور (که به صورت پیش فرض مشخص مـی باشـد)، ارسال می کند. DNS سرور محلی پس از جستجو، آدرس IP معادل با یک نام نمادین را بر می گرداند. تابع تحلیلگر نـام نیز آن آدرس IP را به برنامهٔ کاربردی تحویل می دهد. با پیدا شدن آدرس IP برنامهٔ کـاربردی مـی توانـد عملیـات مـورد نظرش را ادامه بدهد.

[11] Library Function
[12] Name Resolver
[13] Query Packet