1)

1. **DHCP** (پروتکل پیکربندی میزبان پویا): آدرس های IP و پیکربندی شبکه را به صورت پویا به دستگاه ها اختصاص می دهد و اتصال یکپارچه را امکان پذیر می کند.

2. **DNS** (سیستم نام دامنه): نام دامنه (به عنوان مثال، example.com) را به آدرس های IP برای ارتباط دستگاه حل می کند.

3. **HTTP** (پروتکل انتقال ابرمتن): ارتباط بین مرورگرهای وب و سرورها را برای انتقال داده های صفحه وب تسهیل می کند.

2)

1. **TLS (امنیت لایه حمل و نقل):**

- TLS با رمزگذاری داده ها، جلوگیری از رهگیری یا دستکاری، ارتباط ایمن بین سرویس گیرنده و سرور را تضمین می کند. موارد استفاده رایج شامل مرور وب HTTPS است.
- **جزئیات اضافی:**

  - **فریم 1:** این فریم داده های برنامه TLS رمزگذاری شده را نشان می دهد. این نشان می دهد که ارتباط مشتری و سرور به حالتی رسیده است که آنها به طور ایمن در حال تبادل داده ها هستند.
  - **فریم ۱۶:** پیام «سلام مشتری» اولین مرحله از دست دادن TLS است. مشخص می کند:
    - مجموعه های رمزنگاری پشتیبانی شده (الگوریتم های رمزگذاری).
    - نسخه های TLS پشتیبانی شده است.
    - داده های تصادفی برای استقرار جلسه استفاده شد.
    - SNI (نشانگر نام سرور)، که به سرور کمک می کند تا سرویس خاص درخواست شده را هنگام میزبانی چندین سرویس در یک IP شناسایی کند.

2. **TCP (پروتکل کنترل انتقال):**

- TCP ستون فقرات ارتباطات اینترنتی قابل اعتماد است، ارتباطات بین نقاط پایانی را مدیریت می کند و یکپارچگی داده ها را تضمین می کند.
- **جزئیات اضافی:**

  - **فریم 2:** بسته FIN-ACK بخشی از دست دادن چهار طرفه است که برای بستن ظریف اتصال TCP استفاده می شود. این تضمین می کند که تمام داده ها قبل از بسته شدن جلسه منتقل شده اند.
  - **فریم های 10 و 17:** این فریم ها نشان می دهند که چگونه تکه های بزرگی از داده ها برای انتقال تقسیم بندی می شوند. مونتاژ مجدد تضمین می کند که هیچ داده ای در حین انتقال از بین نمی رود.

3. **DNS (سیستم نام دامنه):**

- DNS نام های دامنه قابل خواندن توسط انسان را به آدرس های IP حل می کند و دستگاه ها را قادر می سازد تا سرورها را در اینترنت مکان یابی کنند.
- **جزئیات اضافی:**

- **فریم 6:** پرس و جو به دنبال آدرس IP v20.events.data.microsoft.com است که اغلب برای تله متری یا تجزیه و تحلیل توسط سرویس های مایکروسافت استفاده می شود.
- **فریم 7:** پاسخ چندین آدرس IP را ارائه می دهد. این نشان دهنده یکی از موارد زیر است:
  - تعادل بار: توزیع درخواست ها در چندین سرور.
  - توزیع جغرافیایی: اطمینان از اتصال کاربران به نزدیکترین یا پاسخگوترین سرور.

4 . **اترنت II و IPv4 (لینک و لایه شبکه):**

- فرمت فریم اترنت II و پروتکل IPv4 دستگاه های موجود در شبکه های یکسان و مختلف را قادر می سازد تا با هم ارتباط برقرار کنند.
- **جزئیات اضافی:**

- **فریم 1:** آدرس MAC منبع (fa:7f:1a:d7:93:85) دستگاهی را که بسته را منشا می کند مشخص می کند. MAC مقصد (b4:8c:9d:13:c3:53) دستگاه محلی است.
- آدرس های IPv4 (51.15.22.23 به عنوان منبع و 192.168.67.6 به عنوان مقصد) نقاط پایانی را برای مسیریابی بسته تعریف می کنند.

5 . **وضوح DNS:**

- فرآیند DNS با یک پرس و جو (Frame 6) شروع می شود و با یک پاسخ (Frame 7) به پایان می رسد.
- **بینش گسترده:**

- پاسخ v20.events.data.microsoft.com به چندین آدرس IP حل می شود، احتمالا با استفاده از شبکه تحویل محتوا CDN .(CDN) ها به کاهش تأخیر و افزایش قابلیت اطمینان کمک می کنند.

6 . **دست دادن TLS:**

- فریم هایی مانند 16 ("Client Hello") و 59 ("Client Hello" برای نام میزبان دیگر) نشان دهنده شروع جلسات امن است.
- **بینش گسترده:**

- فیلد SNI در این بسته ها نام میزبان دقیقی را که مشتری قصد برقراری ارتباط با آن را دارد مشخص می کند. این برای سرورهایی که چندین وب سایت را با یک IP میزبانی می کنند بسیار مهم است.

7 . **بخش های داده و مونتاژ مجدد:**

- فریم های 10، 17 و 19 نمونه هایی از فرآیند تقسیم بندی TCP هستند. هر بخش دارای موارد زیر است:

- یک شماره توالی منحصر به فرد، اطمینان حاصل می کند که تمام قسمت های داده ها به ترتیب صحیح مونتاژ می شوند.
- اعداد قدردانی، تأیید دریافت بخش های قبلی.

- **بینش گسترده:**

- فریم 19 یک محموله دوباره مونتاژ شده است که داده های برنامه یا یک پاسخ HTTP رمزگذاری شده را پیشنهاد می کند.

8 . **چرخه عمر اتصال:**

- جلسات TCP با بسته های SYN (فریم های 8 و 14) شروع می شود و با بسته های FIN (فریم های 2 و 4) به پایان می رسد.
- **بینش گسترده:**
  - بسته های SYN یک درخواست اتصال جدید را نشان می دهند.
  - فریم 8 یک بسته SYN را نشان می دهد که به 142.132.181.170 در پورت 443 ارسال شده است و ارتباط HTTPS را آغاز می کند.

9 . **ترافیک HTTP/HTTPS:**

- HTTPS برای رمزگذاری ترافیک وب به TLS متکی است.
- **بینش گسترده:**
  - در حالی که محتویات بسته های HTTPS رمزگذاری شده است، ابرداده هایی مانند IP ها و پورت های منبع/مقصد (به عنوان مثال، فریم 12، 443) سرنخ هایی در مورد ارتباط ارائه می دهند.
  - چندین بسته داده برنامه TLS (به عنوان مثال، فریم 13، 19) انتقال یک محموله بزرگ، احتمالا یک صفحه وب یا محتوای مرتبط را پیشنهاد می کند.