دانشکده مهندسی کامپیوتر

آزمایشگاه شبکه‌های کامپیوتری

گزارش آزمایش سوم

عنوان آزمایش : آشنایی پشرفته با نرم افزار Wireshark

دکتر بردیا صفایی

سارا آذرنوش — ۹۸۱۷۰۶۶۸

کهبد آئینی — ۹۸۱۰۱۲۰۹

پارسا محمدیان — ۹۸۱۰۲۲۸۴

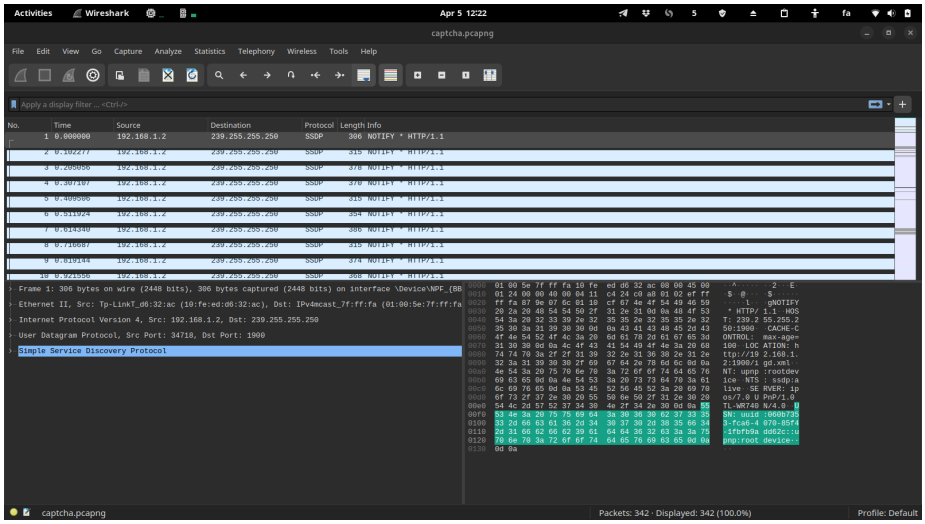
۱۶ اسفند ۱۴۰۲

فهرست مطالب

۱ Wireshark

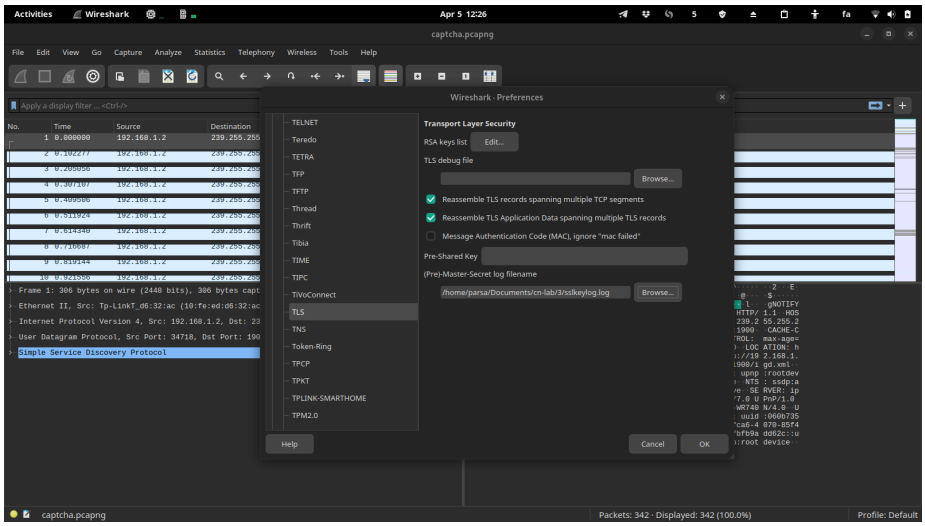
۱.۱ به دست آوردن captcha

۱. همانطور که در شکل زیر مشاهده می‌کنیم،فایل captcha.pcapng را د نرم‌افزار Wireshark باز می‌کنیم.



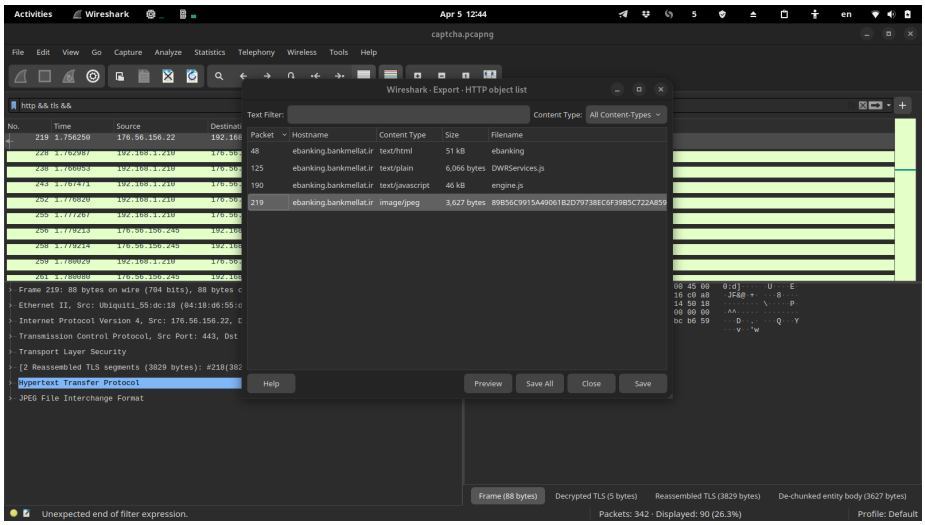
شکل ۱: محتویات فایل captcha.pcapng

۲. سپس فایل کلید جلسه را در قسمت تنظیمات پروتوکل TLS اضافه می‌کنیم.



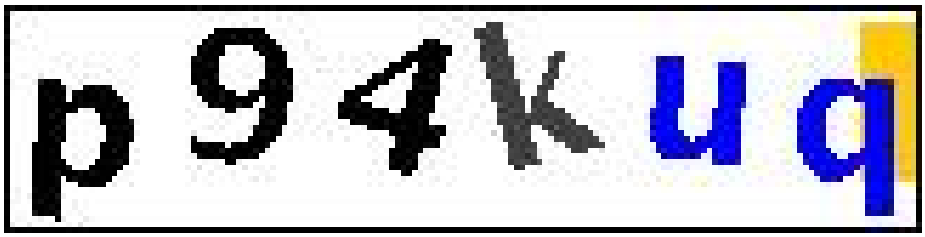
شکل ۲: اضافه کردن کلید جلسه

۳. حال بسته‌های مربوطه را با اعمال فیلتر پیدا می‌کنیم و از قسمت File>Export Objects گزینه HTTP را انتخاب می‌کنیم.



شکل ۳: قسمت Export Objects

۴. فایل عکسی که مربوط به کپچا هست را save می‌کنیم. تصویر مربوط به کپچا در ادامه قابل مشاهده است.



شکل ۴: تصویر captcha

۲.۱ سوال‌ها

۱. اطلاعات آماری در نرم‌افزار Wireshark از منوی بالا، گزینه Statistics به دست می‌آیند. ابزارهای موجود در این منو می‌توانند برای انجام تحلیل‌های مختلف در شبکه به کار گرفته شوند و اطلاعاتی از ساختار درونی شبکه به تحلیل‌گر بدهند. در ادامه هر کدام از آیتم‌های موجود در آن را توضیح می‌دهیم و می‌گوییم به چه کاری می‌آیند.

- Properties File Capture
  اطلاعات مربوط به فایل کپچر فعلی را نمایش می‌دهد.
- Addresses Resolved
  لیست آدرس‌ها و IP های ریزالو شده برای هرکدام را نشان می‌دهد.
- Hierarchy Protocol
  ساختار درختی از پروتکل‌های استفاده شده نشان می‌دهد.
- Conversations
  ترافیک رد و بدل شده بین دو آدرس را نشان می‌دهد.
- Endpoints
  آدرس‌های که به آن‌ها متصل شده‌ایم و آماری در مورد آن‌ها را نشان می‌دهد.
- Lengths Packet
  توزیع طول پکت‌ها را نشان می‌دهد.
- Graphs I/O
  نمودار سری زمانی تعداد بسته‌ها را نمایش می‌دهد.
- Time Response Service
  فاصله زمانی بین درخواست‌ها و پاسخ آن‌ها را نمایش می‌دهد.
- (BOOTP) DHCP
  جدولی شامل اطلاعات پیام‌های DHCP را نمایش می‌دهد.
- NetPerfMeter
  ابزاری برای تست و مشاهده performance است.
- Programs ONC-RPC
  اطلاعاتی راجع به نرم‌افزارهای مختلف و پورت کاری آن‌ها را شامل می‌شود.

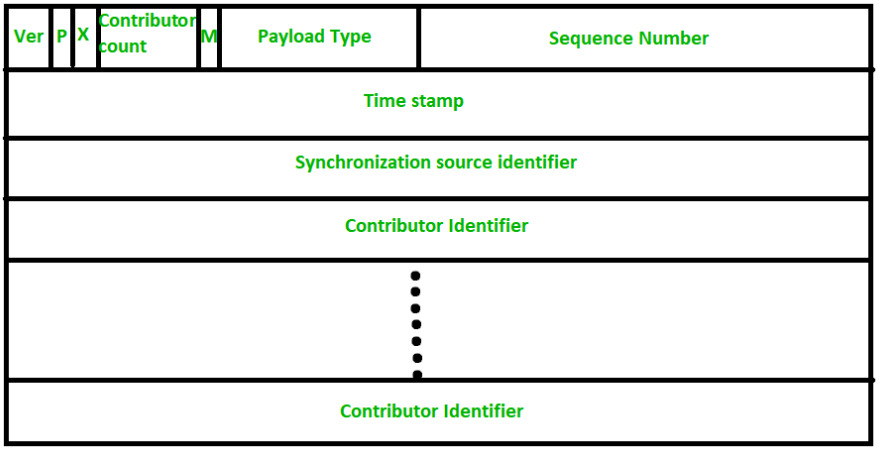
- ۲۹West
اطلاعات مربوط به پروتکلی که برای جابجایی پیام به کار می‌رود را نشان می‌دهد.
- ANCP
اطلاعات مربوط به پروتکلی با همین نام را نشان می‌دهد.
- BACnet
اطلاعات مربوط به پروتکلی با همین نام را نشان می‌دهد.
- Collectd
آمار مربوط به سیستم را جمع آوری می‌کند.
- DNS
اطلاعات مربوط به پیام‌های DNS را نشان می‌دهد.
- Graph Flow
به صورت تصویری اتصالات بین hostها را نشان می‌دهد.
- HART-IP اطلاعات مربوط به پروتکلی با همین نام را نشان می‌دهد.
- HPFEEDS اطلاعات مربوط به پروتکلی با همین نام را نشان می‌دهد.
- HTTP اطلاعات مربوط به پروتکل HTTP را نشان می‌دهد.
- HTTP۲ اطلاعات مربوط به پروتکل HTTP نسخه ۲ را نشان می‌دهد.
- Sametime اطلاعات مربوط به پروتکل HTTP را نشان می‌دهد.
- Graphs Stream TCP
جریان‌های TCP را به صورت بصری نمایش می‌دهد.
- Streams Multicast UDP
اطلاعات مربوط به جریان‌های UDP Multicast را نشان می‌دهد.
- (RSerPool) Pooling Server Reliable
اطلاعات پروتکل‌های مختلف برای RSerPool را نشان می‌دهد.
- F۵
اطلاعات پکت‌ها و بایت‌های مربوط به Virtual Server Distribution و tmm Distribution را نشان می‌دهد.
- Statistics IPv۴
آمار مربوط به پروتکل IP ورژن ۴ را نشان می‌دهد.
- Statistics IPv۶
آمار مربوط به پروتکل IP ورژن ۶ را نشان می‌دهد.

این اطلاعات برای عیب‌یابی لایه‌های مختلف در شبکه کاربرد دارند.

۲. پروتکل RTP یا Real-time Transport Protocol یکی از پروتکل‌های شبکه برای انتقال داده صوتی و تصویری تحت بستر IP است. این پروتکل در زمینه‌های ارتباطات و سیستم‌های سرگرمی چند رسانه‌ای مورد استفاده قرار می‌گیرد.

پروتکل RTP معمولا تحت بستر UDP در کنار پروتکل RTCP یا RTP Control Protocol به کار می‌رود. RTP مسئولیت انتقال جریان داده را دارد در حالی که RTCP مسئولیت مانیتور کردن انتقال را دارد.

در شکل زیر header بسته‌های این پروتکل را مشاهده می‌کنیم.



در نرم‌افزار Wireshark ابزاری برای تحلیل بسته‌های پروتکل RTP وجود دارد که از نوار بالا قسمت Telephony>RTP>RTP Streams قابل دسترس است. در این بخش داده‌های منتقل شده نمایش داده می‌شوند، و امکان پخش کردن آن‌ها و همچنین Export کردن آن‌ها به فایل نیز وجود دارد.