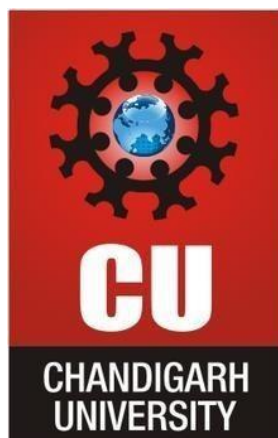




DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

**CHANDIGARH UNIVERSITY
UNIVERSITY INSTITUTE OF ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**



Submitted By: Pranjal Kumar		Submitted To: Renuka Ratten	
Subject Name		WEB AND MOBILE SECURITY LAB	
Subject Code		20CSP-338	
Branch		Computer Science	
Semester		5th	



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

UNIVERSITY INSTITUTE OF ENGINEERING

Department of Computer Science & Engineering

Subject Name: WEB AND MOBILE SECURITY LAB

Subject Code: 20CSP-338

Submitted to: Renuka Ratten

Submitted by: Pranjal Kumar

Faculty name: Renuka Ratten

Name: Pranjal Kumar

UID: 20BCS3504

Section: 607

Group: B

Ex. No	List of Experiments	Date	Conduct (MM: 12)	Viva (MM: 10)	Record (MM: 8)	Total (MM: 30)	Remarks/Signature
1.1	Open any website on computer system and identify http packet on monitoring tool like Wireshark.	19/08/22					
1.2	Design a method to simulate the html injection and cross sites scripting to exploit the attackers	28/08/22					
1.3	Working of CSRF (cross site request forgery) attack/ Vulnerability.	16/09/22					
2.1	Design methods to break authentication schemes (SQL Injection Attack).	04/09/22					
2.2							
2.3							
2.4							
3.1							

3.2							
3.3							

Experiment No 1

Aim: Open any website on computer system and identify http packet on monitoring tool like Wireshark

Objective: To analyse Http traffic

Software/Hardware Requirements: Windows 7 & above version

Tools to be used: Wireshark App

Introduction: Wireshark is a software tool used to monitor the network traffic through a network interface. It is the most widely used network monitoring tool today. Wireshark is loved equally by system administrators, network engineers, network enthusiasts, network security professionals and black hat hackers.

The extent of its popularity is such, that experience with Wireshark is considered as a valuable/essential trait in a computer networking-related professional.

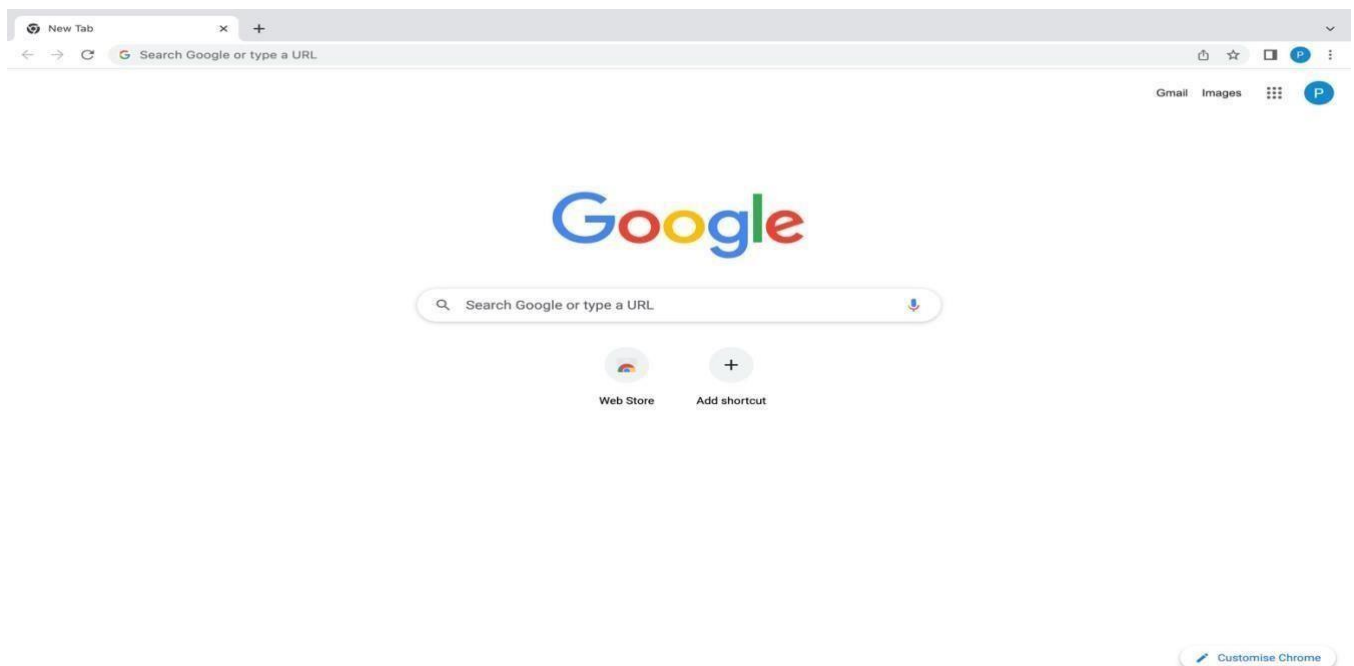
Steps/Method/Coding:

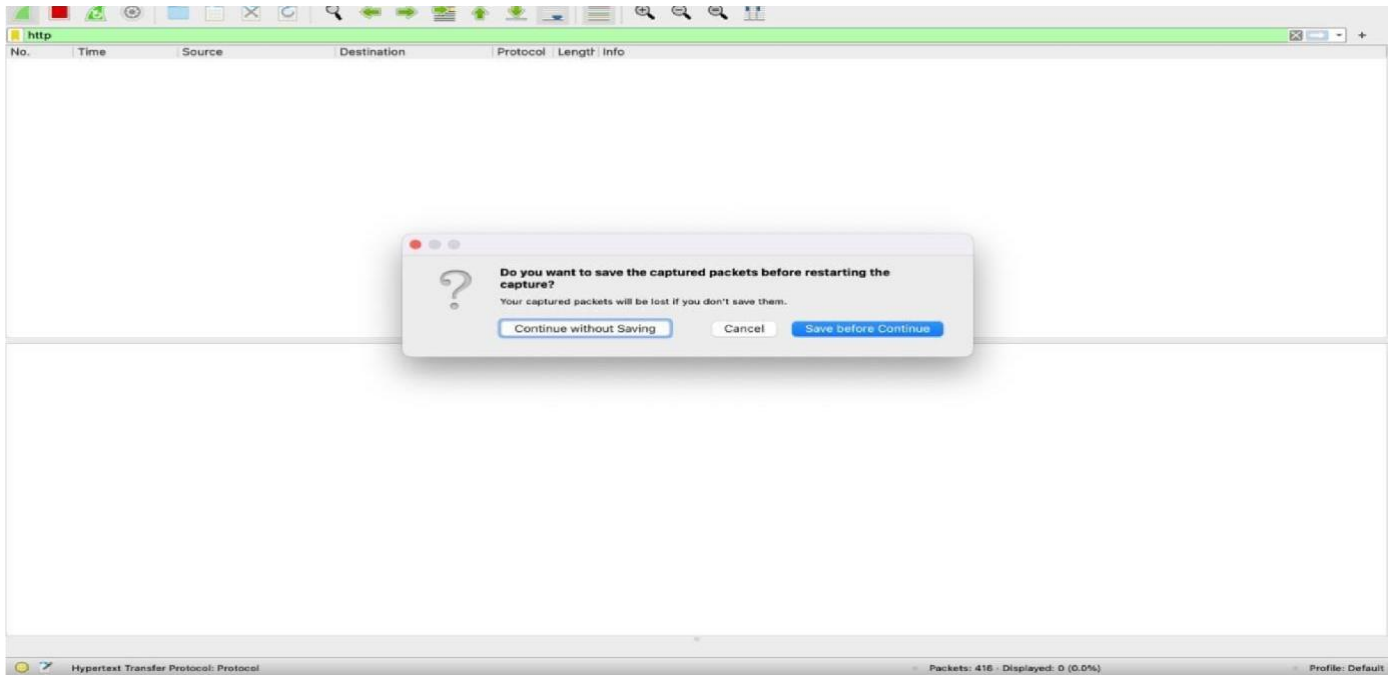
1. Install Wireshark.
2. Open your Internet browser.
3. Clear your browser cache.
4. Open Wireshark

5. Click on "Capture > Interfaces". A pop-up window will display.
6. You'll want to capture traffic that goes through your ethernet driver. Click on the Start button to capture traffic via this interface.
7. Visit the URL that you wanted to capture the traffic from.
8. Go back to your Wireshark screen and press Ctrl + E to stop capturing.
9. After the traffic capture is stopped, please save the captured traffic into a *.pcap format file and attach it to your support ticket.

Output screenshot:

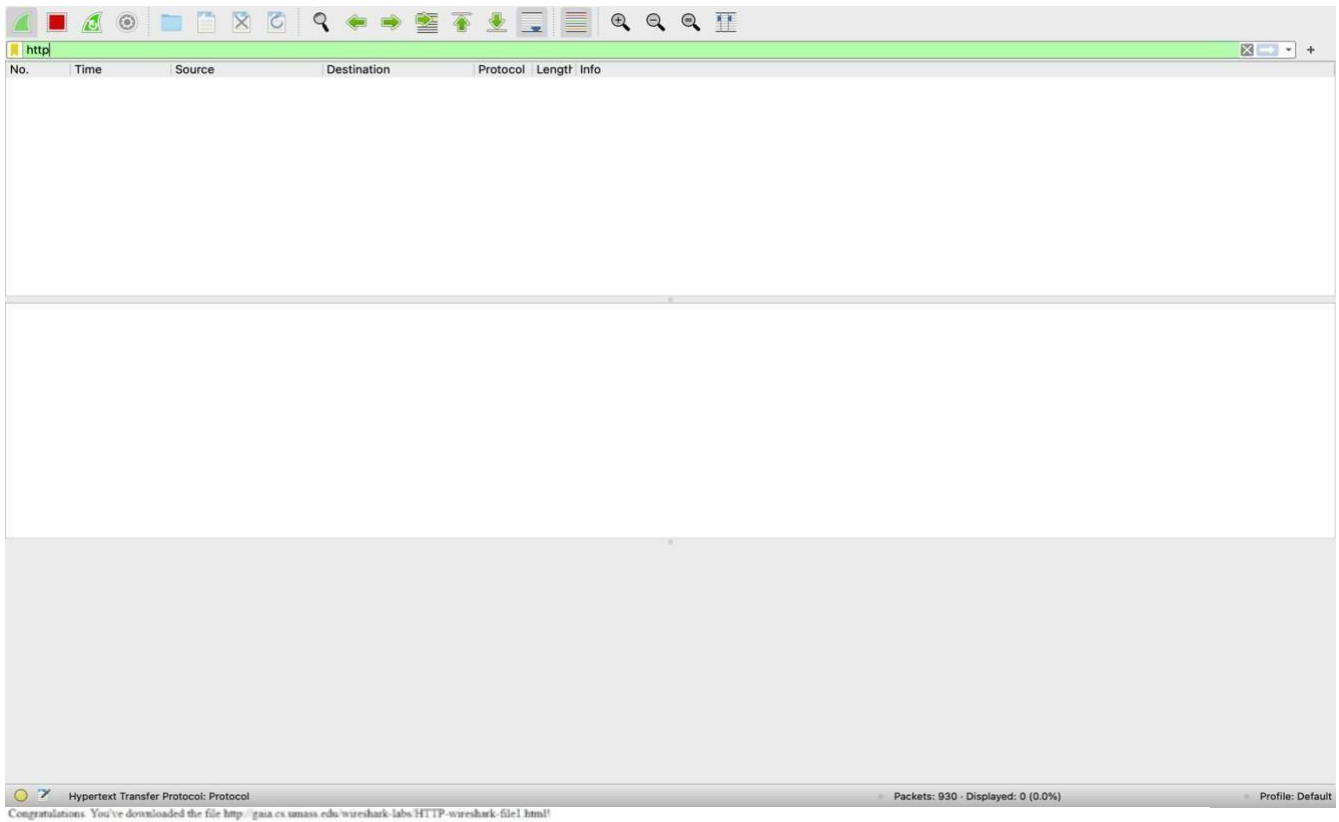
before doing any other activities I will clear the cache of my browser





link

and
then I will open a



The link:

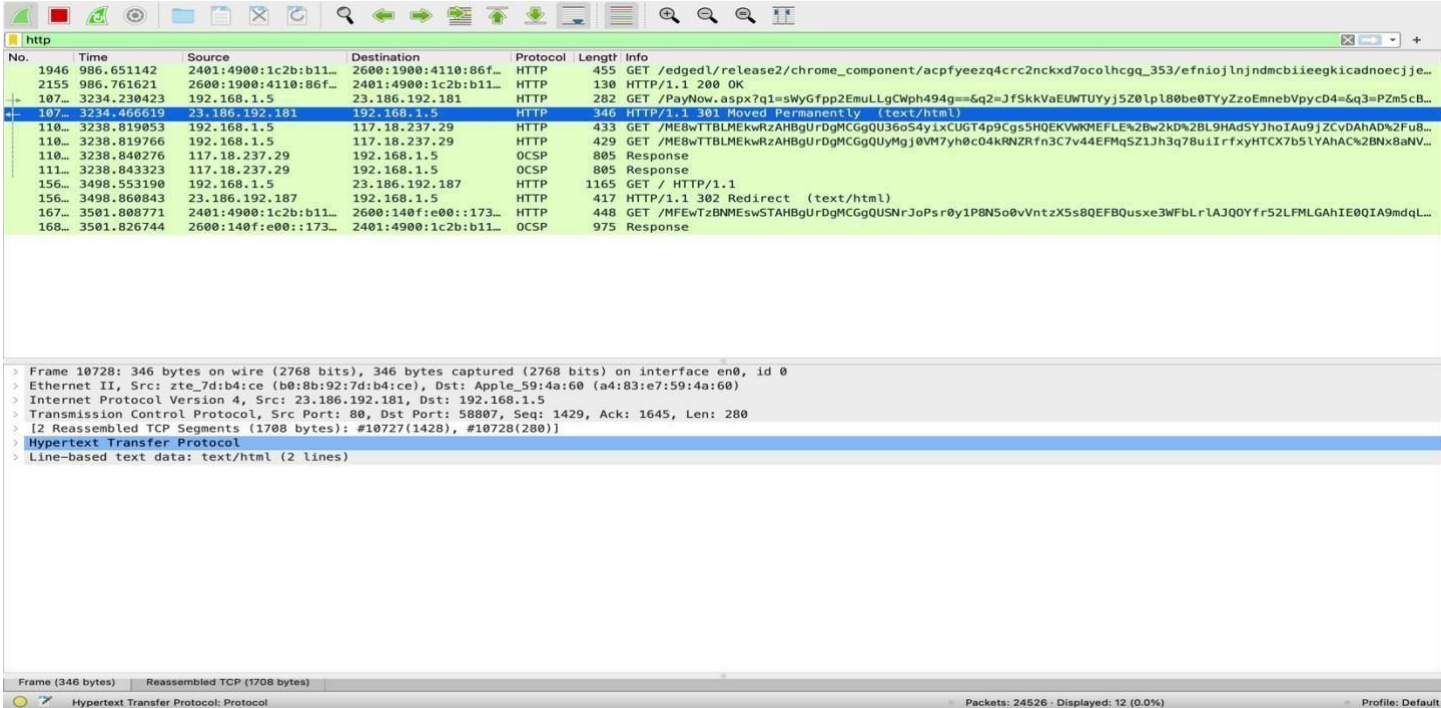
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>



http

No.	Time	Source	Destination	Protocol	Length	Info
1946	986.651142	2401:4900:1c2b:b11...	2600:1900:4110:86f...	HTTP	455	GET /edgedl/release2/chrome_component/acpfyeezq4crc2nckxd7ocolhcgq_353/efniojlnjndmcbiieegkicadnoecjie...
2155	986.761621	2600:1900:4110:86f...	2401:4900:1c2b:b11...	HTTP	130	HTTP/1.1 200 OK
107...	3234.230423	192.168.1.5	23.186.192.181	HTTP	282	GET /PayNow.aspx?q1=sWyGfpp2EmuLLgCWph494g==6q2=JfSkkVaEUWUYy5Z0lp180be0TYyZzoEmnebVpypcD4=&q3=PZm5cB...
107...	3234.466619	23.186.192.181	192.168.1.5	HTTP	346	HTTP/1.1 301 Moved Permanently (text/html)
110...	3238.819053	192.168.1.5	117.18.237.29	HTTP	433	GET /ME8wTTBLMEkWRzAHBgUrDgMCGgQU36o54yixCUGT4p9Cgs5HQEKVWkMEFLE%2Bw2kD%2BL9HAdSYJhoIAu9jZCvDAhAd%2Fu8...
110...	3238.819766	192.168.1.5	117.18.237.29	HTTP	429	GET /ME8wTTBLMEkWRzAHBgUrDgMCGgQUyMgj0VM7yh0c04kRNZRfn3C7v44EFMqSZ1jh3q78uiIrfxyHTCX7b5LYAhAC%2BNx8aNV...
110...	3238.840276	117.18.237.29	192.168.1.5	OCSP	805	Response
111...	3238.843323	117.18.237.29	192.168.1.5	OCSP	805	Response
156...	3498.553190	192.168.1.5	23.186.192.187	HTTP	1165	GET / HTTP/1.1
156...	3498.800843	23.186.192.187	192.168.1.5	HTTP	417	HTTP/1.1 302 Redirect (text/html)
167...	3501.800871	2401:4900:1c2b:b11...	2600:140f:e00:173...	HTTP	448	GET /MFEwT2BNMEswSTAHBgUrDgMCGgQUUSNrJoPr0y1P8N5o0vVntzX5s8QEFBQusxe3WfBLrLAJQ0Yfr52LFMLGAhIE0QIA9mdqL...
168...	3501.826744	2600:140f:e00:173...	2401:4900:1c2b:b11...	OCSP	975	Response

> Frame 2155: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface en0, id 0
 > Ethernet II, Src: zte_7d:b4:ce (b0:8b:92:7d:b4:ce), Dst: Apple_59:4a:60 (a4:83:e7:59:4a:60)
 > Internet Protocol Version 6, Src: 2600:1900:4110:86f::, Dst: 2401:4900:1c2b:b116:55ea:d6c2:1714:abc2
 > Transmission Control Protocol, Src Port: 80, Dst Port: 58730, Seq: 159457, Ack: 370, Len: 44
 > [133 Reassembled TCP Segments (159500 bytes): #1948(1208), #1949(1208), #1950(1208), #1951(1208), #1952(1208), #1954(1208), #1955(1208), #1956(1208), #1957(1208), #1958(1208), #1964(1208), #1965(1208), #1966(1208), #1967(1208), #1968(1208), #1969(1208), #1970(1208), #1971(1208), #1972(1208), #1973(1208), #1974(1208), #1975(1208), #1976(1208), #1977(1208), #1978(1208), #1979(1208), #1980(1208), #1981(1208), #1982(1208), #1983(1208), #1984(1208), #1985(1208), #1986(1208), #1987(1208), #1988(1208), #1989(1208), #1990(1208), #1991(1208), #1992(1208), #1993(1208), #1994(1208), #1995(1208), #1996(1208), #1997(1208), #1998(1208), #1999(1208), #2000(1208), #2001(1208), #2002(1208), #2003(1208), #2004(1208), #2005(1208), #2006(1208), #2007(1208), #2008(1208), #2009(1208), #2010(1208), #2011(1208), #2012(1208), #2013(1208), #2014(1208), #2015(1208), #2016(1208), #2017(1208), #2018(1208), #2019(1208), #2020(1208), #2021(1208), #2022(1208), #2023(1208), #2024(1208), #2025(1208), #2026(1208), #2027(1208), #2028(1208), #2029(1208), #2030(1208), #2031(1208), #2032(1208), #2033(1208), #2034(1208), #2035(1208), #2036(1208), #2037(1208), #2038(1208), #2039(1208), #2040(1208), #2041(1208), #2042(1208), #2043(1208), #2044(1208), #2045(1208), #2046(1208), #2047(1208), #2048(1208), #2049(1208), #2050(1208), #2051(1208), #2052(1208), #2053(1208), #2054(1208), #2055(1208), #2056(1208), #2057(1208), #2058(1208), #2059(1208), #2060(1208), #2061(1208), #2062(1208), #2063(1208), #2064(1208), #2065(1208), #2066(1208), #2067(1208), #2068(1208), #2069(1208), #2070(1208), #2071(1208), #2072(1208), #2073(1208), #2074(1208), #2075(1208), #2076(1208), #2077(1208), #2078(1208), #2079(1208), #2080(1208), #2081(1208), #2082(1208), #2083(1208), #2084(1208), #2085(1208), #2086(1208), #2087(1208), #2088(1208), #2089(1208), #2090(1208), #2091(1208), #2092(1208), #2093(1208), #2094(1208), #2095(1208), #2096(1208), #2097(1208), #2098(1208), #2099(1208), #2100(1208), #2101(1208), #2102(1208), #2103(1208), #2104(1208), #2105(1208), #2106(1208), #2107(1208), #2108(1208), #2109(1208), #2110(1208), #2111(1208), #2112(1208), #2113(1208), #2114(1208), #2115(1208), #2116(1208), #2117(1208), #2118(1208), #2119(1208), #2120(1208), #2121(1208), #2122(1208), #2123(1208), #2124(1208), #2125(1208), #2126(1208), #2127(1208), #2128(1208), #2129(1208), #2130(1208), #2131(1208), #2132(1208), #2133(1208), #2134(1208), #2135(1208), #2136(1208), #2137(1208), #2138(1208), #2139(1208), #2140(1208), #2141(1208), #2142(1208), #2143(1208), #2144(1208), #2145(1208), #2146(1208), #2147(1208), #2148(1208), #2149(1208), #2150(1208), #2151(1208), #2152(1208), #2153(1208), #2154(1208), #2155(1208), #2156(1208), #2157(1208), #2158(1208), #2159(1208), #2160(1208), #2161(1208), #2162(1208), #2163(1208), #2164(1208), #2165(1208), #2166(1208), #2167(1208), #2168(1208), #2169(1208), #2170(1208), #2171(1208), #2172(1208), #2173(1208), #2174(1208), #2175(1208), #2176(1208), #2177(1208), #2178(1208), #2179(1208), #2180(1208), #2181(1208), #2182(1208), #2183(1208), #2184(1208), #2185(1208), #2186(1208), #2187(1208), #2188(1208), #2189(1208), #2190(1208), #2191(1208), #2192(1208), #2193(1208), #2194(1208), #2195(1208), #2196(1208), #2197(1208), #2198(1208), #2199(1208), #2200(1208), #2201(1208), #2202(1208), #2203(1208), #2204(1208), #2205(1208), #2206(1208), #2207(1208), #2208(1208), #2209(1208), #2210(1208), #2211(1208), #2212(1208), #2213(1208), #2214(1208), #2215(1208), #2216(1208), #2217(1208), #2218(1208), #2219(1208), #2220(1208), #2221(1208), #2222(1208), #2223(1208), #2224(1208), #2225(1208), #2226(1208), #2227(1208), #2228(1208), #2229(1208), #2230(1208), #2231(1208), #2232(1208), #2233(1208), #2234(1208), #2235(1208), #2236(1208), #2237(1208), #2238(1208), #2239(1208), #2240(1208), #2241(1208), #2242(1208), #2243(1208), #2244(1208), #2245(1208), #2246(1208), #2247(1208), #2248(1208), #2249(1208), #2250(1208), #2251(1208), #2252(1208), #2253(1208), #2254(1208), #2255(1208), #2256(1208), #2257(1208), #2258(1208), #2259(1208), #2260(1208), #2261(1208), #2262(1208), #2263(1208), #2264(1208), #2265(1208), #2266(1208), #2267(1208), #2268(1208), #2269(1208), #2270(1208), #2271(1208), #2272(1208), #2273(1208), #2274(1208), #2275(1208), #2276(1208), #2277(1208), #2278(1208), #2279(1208), #2280(1208), #2281(1208), #2282(1208), #2283(1208), #2284(1208), #2285(1208), #2286(1208), #2287(1208), #2288(1208), #2289(1208), #2290(1208), #2291(1208), #2292(1208), #2293(1208), #2294(1208), #2295(1208), #2296(1208), #2297(1208), #2298(1208), #2299(1208), #2300(1208), #2301(1208), #2302(1208), #2303(1208), #2304(1208), #2305(1208), #2306(1208), #2307(1208), #2308(1208), #2309(1208), #2310(1208), #2311(1208), #2312(1208), #2313(1208), #2314(1208), #2315(1208), #2316(1208), #2317(1208), #2318(1208), #2319(1208), #2320(1208), #2321(1208), #2322(1208), #2323(1208), #2324(1208), #2325(1208), #2326(1208), #2327(1208), #2328(1208), #2329(1208), #2330(1208), #2331(1208), #2332(1208), #2333(1208), #2334(1208), #2335(1208), #2336(1208), #2337(1208), #2338(1208), #2339(1208), #2340(1208), #2341(1208), #2342(1208), #2343(1208), #2344(1208), #2345(1208), #2346(1208), #2347(1208), #2348(1208), #2349(1208), #2350(1208), #2351(1208), #2352(1208), #2353(1208), #2354(1208), #2355(1208), #2356(1208), #2357(1208), #2358(1208), #2359(1208), #2360(1208), #2361(1208), #2362(1208), #2363(1208), #2364(1208), #2365(1208), #2366(1208), #2367(1208), #2368(1208), #2369(1208), #2370(1208), #2371(1208), #2372(1208), #2373(1208), #2374(1208), #2375(1208), #2376(1208), #2377(1208), #2378(1208), #2379(1208), #2380(1208), #2381(1208), #2382(1208), #2383(1208), #2384(1208), #2385(1208), #2386(1208), #2387(1208), #2388(1208), #2389(1208), #2390(1208), #2391(1208), #2392(1208), #2393(1208), #2394(1208), #2395(1208), #2396(1208), #2397(1208), #2398(1208), #2399(1208), #2400(1208), #2401(1208), #2402(1208), #2403(1208), #2404(1208), #2405(1208), #2406(1208), #2407(1208), #2408(1208), #2409(1208), #2410(1208), #2411(1208), #2412(1208), #2413(1208), #2414(1208), #2415(1208), #2416(1208), #2417(1208), #2418(1208), #2419(1208), #2420(1208), #2421(1208), #2422(1208), #2423(1208), #2424(1208), #2425(1208), #2426(1208), #2427(1208), #2428(1208), #2429(1208), #2430(1208), #2431(1208), #2432(1208), #2433(1208), #2434(1208), #2435(1208), #2436(1208), #2437(1208), #2438(1208), #2439(1208), #2440(1208), #2441(1208), #2442(1208), #2443(1208), #2444(1208), #2445(1208), #2446(1208), #2447(1208), #2448(1208), #2449(1208), #2450(1208), #2451(1208), #2452(1208), #2453(1208), #2454(1208), #2455(1208), #2456(1208), #2457(1208), #2458(1208), #2459(1208), #2460(1208), #2461(1208), #2462(1208), #2463(1208), #2464(1208), #2465(1208), #2466(1208), #2467(1208), #2468(1208), #2469(1208), #2470(1208), #2471(1208), #2472(1208), #2473(1208), #2474(1208), #2475(1208), #2476(1208), #2477(1208), #2478(1208), #2479(1208), #2480(1208), #2481(1208), #2482(1208), #2483(1208), #2484(1208), #2485(1208), #2486(1208), #2487(1208), #2488(1208), #2489(1208), #2490(1208), #2491(1208), #2492(1208), #2493(1208), #2494(1208), #2495(1208), #2496(1208), #2497(1208), #2498(1208), #2499(1208), #2500(1208), #2501(1208), #2502(1208), #2503(1208), #2504(1208), #2505(1208), #2506(1208), #2507(1208), #2508(1208), #2509(1208), #2510(1208), #2511(1208), #2512(1208), #2513(1208), #2514(1208), #2515(1208), #2516(1208), #2517(1208), #2518(1208), #2519(1208), #2520(1208), #2521(1208), #2522(1208), #2523(1208), #2524(1208), #2525(1208), #2526(1208), #2527(1208), #2528(1208), #2529(1208), #2530(1208), #2531(1208), #2532(1208), #2533(1208), #2534(1208), #2535(1208), #2536(1208), #2537(1208), #2538(1208), #2539(1208), #2540(1208), #2541(1208), #2542(1208), #2543(1208), #2544(1208), #2545(1208), #2546(1208), #2547(1208), #2548(1208), #2549(1208), #2550(1208), #2551(1208), #2552(1208), #2553(1208), #2554(1208), #2555(1208), #2556(1208), #2557(1208), #2558(1208), #2559(1208), #2560(1208), #2561(1208), #2562(1208), #2563(1208), #2564(1208), #2565(1208), #2566(1208), #2567(1208), #2568(1208), #2569(1208), #2570(1208), #2571(1208), #2572(1208), #2573(1208), #2574(1208), #2575(1208), #2576(1208), #2577(1208), #2578(1208), #2579(1208), #2580(1208), #2581(1208), #2582(1208), #2583(1208), #2584(1208), #2585(1208), #2586(1208), #2587(1208), #2588(1208), #2589(1208), #2590(1208), #2591(1208), #2592(1208), #2593(1208), #2594(1208), #2595(1208), #2596(1208), #2597(1208), #2598(1208), #2599(1208), #2600(1208), #2601(1208), #2602(1208), #2603(1208), #2604(1208), #2605(1208), #2606(1208), #2607(1208), #2608(1208), #2609(1208), #2610(1208), #2611(1208), #2612(1208), #2613(1208), #2614(1208), #2615(1208), #2616(1208), #2617(1208), #2618(1208), #2619(1208), #2620(1208), #2621(1208), #2622(1208), #2623(1208), #2624(1208), #2625(1208), #2626(1208), #2627(1208), #2628(1208), #2629(1208), #2630(1208), #2631(1208), #2632(1208), #2633(1208), #2634(1208), #2635(1208), #2636(1208), #2637(1208), #2638(1208), #2639(1208), #2640(1208), #2641(1208), #2642(1208), #2643(1208), #2644(1208), #2645(1208), #2646(1208), #2647(1208), #2648(1208), #2649(1208), #2650(1208), #2651(1208), #2652(1208), #2653(1208), #2654(1208), #2655(1208), #2656(1208), #2657(1208), #2658(1208), #2659(1208), #2660(1208), #2661(1208), #2662(1208), #2663(1208), #2664(1208), #2665(1208), #2666(1208), #2667(1208), #2668(1208), #2669(1208), #2670(1208), #2671(1208), #2672(1208), #2673(1208), #2674(1208), #2675(1208), #2676(1208), #2677(1208), #2678(1208), #2679(1208), #2680(1208), #2681(1208), #2682(1208), #2683(1208), #2684(1208), #2685(1208), #2686(1208), #2687(1208), #2688(1208), #2689(1208), #2690(1208), #2691(1208), #2692(1208), #2693(1208), #2694(1208), #2695(1208), #2696(1208), #2697(1208), #2698(1208), #2699(1208), #2700(1208), #2701(1208), #2702(1208), #2703(1208), #2704(1208), #2705(1208), #2706(1208), #2707(1208), #2708(1208), #2709(1208), #2710(1208), #2711(1208), #2712(1208), #2713(1208), #2714(1208), #2715(1208), #2716(1208), #2717(1208), #2718(1208), #2719(1208), #2720(1208), #2721(1208), #2722(1208), #2723(1208), #2724(1208), #2725(1208), #2726(1208), #2727(1208), #2728(1208), #2729(1208), #2730(1208), #2731(1208), #2732(1208), #2733(1208), #2734(1208), #2735(1208), #2736(1208), #2737(1208), #2738(1208), #2739(1208), #2740(1208), #2741(1208), #2742(1208), #2743(1208), #2744(1208), #2745(1208), #2746(1208), #2747(1208), #2748(1208), #2749(1208), #2750(1208), #2751(1208), #2752(1208), #2753(1208), #2754(1208), #2755(1208), #2756(1208), #2757(1208), #2758(1208), #2759(1208), #2760(1208), #2761(1208), #2762(1208), #2763(1208), #2764(1208), #2765(1208), #2766(1208), #2767(1208), #2768(1208), #2769(1208), #2770(1208), #2771(1208), #2772(1208), #2773(1208), #2774(1208), #2775(1208), #2776(1208), #2777(1208), #2778(1208), #2779(1208), #2780(1208), #2781(1208), #2782(1208), #2783(1208), #2784(1208), #2785(1208), #2786(1208), #2787(1208), #2788(1208), #2789(1208), #2790(1208), #2791(1208), #2792(1208), #2793(1208), #2794(1208), #2795(1208), #2796(1208), #2797(1208), #2798(1208), #2799(1208), #2800(1208), #2801(1208), #2802(1208), #2803(1208), #2804(1208), #2805(1208), #2806(1208), #2807(1208), #2808(1208), #2809(1208), #2810(1208), #2811(1208), #2812(1208), #2813(1208), #2814(1208), #2815(1208), #2816(1208), #2817(1208), #2818(1208), #2819(1208), #2820(1208), #2821(1208), #2822(1208), #2823(1208), #2824(1208), #2825(1208), #2826(1208), #2827(1208), #2828(1208), #2829(1208), #2830(1208), #2831(1208), #2832(1208), #2833(1208), #2834(1208), #2835(1208), #2836(1208), #2837(1208), #2838(1208), #2839(1208), #2840(1208), #2841(1208), #2842(1208), #2843(1208), #2844(1208), #2845(1208), #2846(1208), #2847(1208), #2848(1208), #2849(1208), #2850(1208), #2851(1208), #2852(1208), #2853(1208), #2854(1208), #2855(1208), #2856(1208), #2857(1208), #2858(1208), #2859(1208), #2860(1208), #2861(1208), #2862(1208), #2863(1208), #2864(1208), #2865(1208), #2866(1208), #2867(1208), #2868(1208), #2869(1208), #2870(1208), #2871(1208), #2872(1208), #2873(1208), #2874(1208), #2875(1208), #2876(1208), #2877(1208), #2878(1208), #2879(1208), #2880(1208), #2881(1208), #2882(1208), #2883(1208), #2884(1208), #2885(1208), #2886(1208), #2887(1208), #2888(1208), #2889(1208), #289

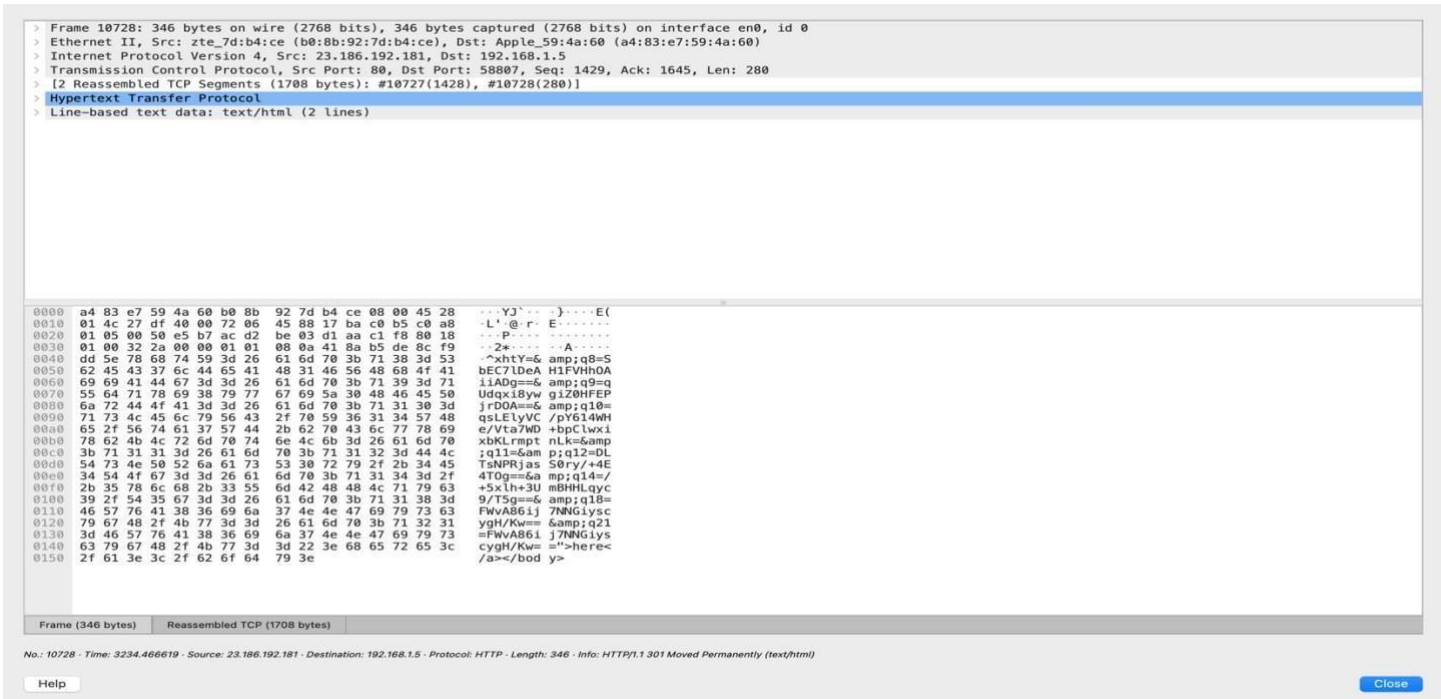


The screenshot shows a Wireshark capture of an HTTP GET request. The packet list on the left shows packet 107 selected. The packet details pane on the right shows the structure of the HTTP request, including the status line: 301 Moved Permanently (text/html). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1946	986.651142	2401:4900:1c2b:b11...	2600:1900:4110:86f...	HTTP	455	GET /edgedl/release2/chrome_component/acpfyeezq4crc2nckxd7oco/hcgq_353/efniojlnjndmcbiieegkicadnoecjje...
2155	986.761621	2600:1900:4110:86f...	2401:4900:1c2b:b11...	HTTP	130	HTTP/1.1 200 OK
107	3234.230423	192.168.1.5	23.186.192.181	HTTP	282	GET /PayNow.aspx?g1=sWyGfpp2EmuLgCwph494g==&q2=Jf5kkVaEUWUyYj5Z0lp180be0TYyZzoEmnebVpycD4=6q3=PZm5CB...
107	3234.466619	23.186.192.181	192.168.1.5	HTTP	346	HTTP/1.1 301 Moved Permanently (text/html)

Frame 10728: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) on interface en0, id 0
 Ethernet II, Src: zte_7d:b4:ce (b0:8b:92:7d:b4:ce), Dst: Apple_59:4a:60 (a4:83:e7:59:4a:60)
 Internet Protocol Version 4, Src: 23.186.192.181, Dst: 192.168.1.5
 Transmission Control Protocol, Src Port: 80, Dst Port: 58807, Seq: 1429, Ack: 1645, Len: 280
 [2 Reassembled TCP Segments (1708 bytes): #10727(1428), #10728(280)]
 Hypertext Transfer Protocol
 Line-based text data: text/html (2 lines)

Frame (346 bytes) | Reassembled TCP (1708 bytes) | Packets: 24526 · Displayed: 12 (0.0%) | Profile: Default



The screenshot shows the hex view of the selected packet in Wireshark. The left pane shows the raw data in hexadecimal, and the right pane shows the corresponding ASCII text. The text is a 301 Moved Permanently redirect response.

```

0000 a4 83 e7 59 4a 60 b0 8b 92 7d b4 ce 08 00 45 28  --YJ'... )....E(
0010 01 4c 27 df 40 00 72 06 45 88 17 ba c0 b5 c0 a8  --L'@:r' E.....
0020 01 05 00 50 e5 b7 ac d2 be 03 d1 aa c1 f8 80 18  --P.....
0030 01 00 32 2a 00 00 01 01 00 0a 41 8a b5 de 8c f9  --Z*.....A.....
0040 dd 5e 70 68 74 59 3d 26 61 6d 70 3b 71 38 3d 53  ^xhtY=5 amp;q8=S
0050 62 45 43 37 6c 44 65 41 48 31 46 56 48 68 4f 41  bEC7LDeA H1FVh0A
0060 69 69 41 44 67 3d 3d 26 61 6d 70 3b 71 39 3d 71  iIADg==6 amp;q9=q
0070 55 64 71 78 69 38 79 77 67 69 5a 30 48 46 45 50  UdqxI8yw giZ0HFEP
0080 6a 72 44 4f 41 3d 3d 26 61 6d 70 3b 71 31 30 3d  jrD0A==6 amp;q10=
0090 71 73 4c 45 6c 79 56 43 2f 70 59 36 31 34 57 48  qsLElyVC /pY614WH
00a0 65 2f 56 74 61 37 57 44 2b 62 70 43 6c 77 78 69  e/Vta7wD +bpClwxI
00b0 78 62 4b 4c 72 6d 70 74 6e 4c 6b 3d 26 61 6d 70  xbxKLmp1 nLk=&amp;
00c0 3b 71 31 31 3d 26 61 6d 70 3b 71 31 32 3d 44 4c  ;q11=&am p;q12=DL
00d0 54 73 4e 50 52 6a 61 73 53 30 72 79 2f 2b 34 45  TsNPRjas S0ry/+4E
00e0 34 54 4f 67 3d 3d 26 61 6d 70 3b 71 31 34 3d 2f  4T0g==6a mp;q14=/
00f0 2b 35 78 6c 68 2b 33 55 6d 42 48 48 4c 71 79 63  +5x1h+3U mBHHLqyc
0100 39 2f 54 35 67 3d 3d 26 61 6d 70 3b 71 31 38 3d  9/TSg==6 amp;q18=
0110 46 57 76 41 38 36 69 6a 37 4e 4e 47 69 79 73 63  FwvA86ij 7NNGlysc
0120 79 67 48 2f 4b 77 3d 3d 26 61 6d 70 3b 71 32 31  ygh/Kw==&amp;q21
0130 3d 46 57 76 41 38 36 69 6a 37 4e 4e 47 69 79 73  =FwvA86i j7NNGlys
0140 63 79 67 48 2f 4b 77 3d 3d 26 3e 68 65 72 65 3c  cygh/Kw=">here<
0150 2f 61 3e 3c 2f 62 6f 64 79 3e  --a></bod y>
  
```

Frame (346 bytes) | Reassembled TCP (1708 bytes)

No.: 10728 · Time: 3234.466619 · Source: 23.186.192.181 · Destination: 192.168.1.5 · Protocol: HTTP · Length: 346 · Info: HTTP/1.1 301 Moved Permanently (text/html)

Help | Close

No.	Time	Source	Destination	Protocol	Length	Info
1946	986.651142	2401:4900:1c2b:b11...	2600:1900:4110:86f...	HTTP	455	GET /edgedl/release2/chrome_component/acpfyeezq4crc2nckxd7oco1hcgq_353/efniojlnjndmcbiieegkicadnoecjje...
2155	986.761621	2600:1900:4110:86f...	2401:4900:1c2b:b11...	HTTP	130	HTTP/1.1 200 OK
107...	3234.230423	192.168.1.5	23.186.192.181	HTTP	282	GET /PayNow.aspx?q1=skYgfp2EmuLgCWph494g==6q2=JfSkkVaEUWUYy5Z0lp180be0TYyZzoEmnebVpycD4=6q3=PZm5cB...
107...	3234.466619	23.186.192.181	192.168.1.5	HTTP	346	HTTP/1.1 301 Moved Permanently (text/html)
110...	3238.819053	192.168.1.5	117.18.237.29	HTTP	433	GET /ME8wTTBLMEkwRzAHBgUrdgMCGgQU36o54yixCUGT4p9Cgs5H0EKVWMEFLE%2Bw2kd%2BL9HAdSYJhoIAu9jZCvDAHAD%2Fu8...
110...	3238.819766	192.168.1.5	117.18.237.29	HTTP	429	GET /ME8wTTBLMEkwRzAHBgUrdgMCGgQU36o54yixCUGT4p9Cgs5H0EKVWMEFLE%2Bw2kd%2BL9HAdSYJhoIAu9jZCvDAHAD%2Fu8...
110...	3238.840276	117.18.237.29	192.168.1.5	OCSP	805	Response
111...	3238.843323	117.18.237.29	192.168.1.5	OCSP	805	Response
156...	3498.000043	192.168.1.5	23.186.192.187	HTTP	1165	GET / HTTP/1.1
156...	3498.000043	23.186.192.187	192.168.1.5	HTTP	417	HTTP/1.1 302 Redirect (text/html)
167...	3501.808771	2401:4900:1c2b:b11...	2600:140f:e00::173...	HTTP	448	GET /MFEWTzBNMEswSTAHBgUrdgMCGgQU5NrJoPsR0y1P8N5o0vVntzX5s8QEFBQusxe3WfBlrLAJQ0Yfr52LFMLGAhIE0QIA9mdqL...
168...	3501.826744	2600:140f:e00::173...	2401:4900:1c2b:b11...	OCSP	975	Response

> Frame 15653: 1165 bytes on wire (9320 bits), 1165 bytes captured (9320 bits) on interface en0, id 0
 > Ethernet II, Src: Apple_59:4a:60 (a4:83:e7:59:4a:60), Dst: zte_7d:b4:ce (b0:8b:92:7d:b4:ce)
 > Internet Protocol Version 4, Src: 192.168.1.5, Dst: 23.186.192.187
 > Transmission Control Protocol, Src Port: 58843, Dst Port: 80, Seq: 1, Ack: 1, Len: 1099
 > Hypertext Transfer Protocol

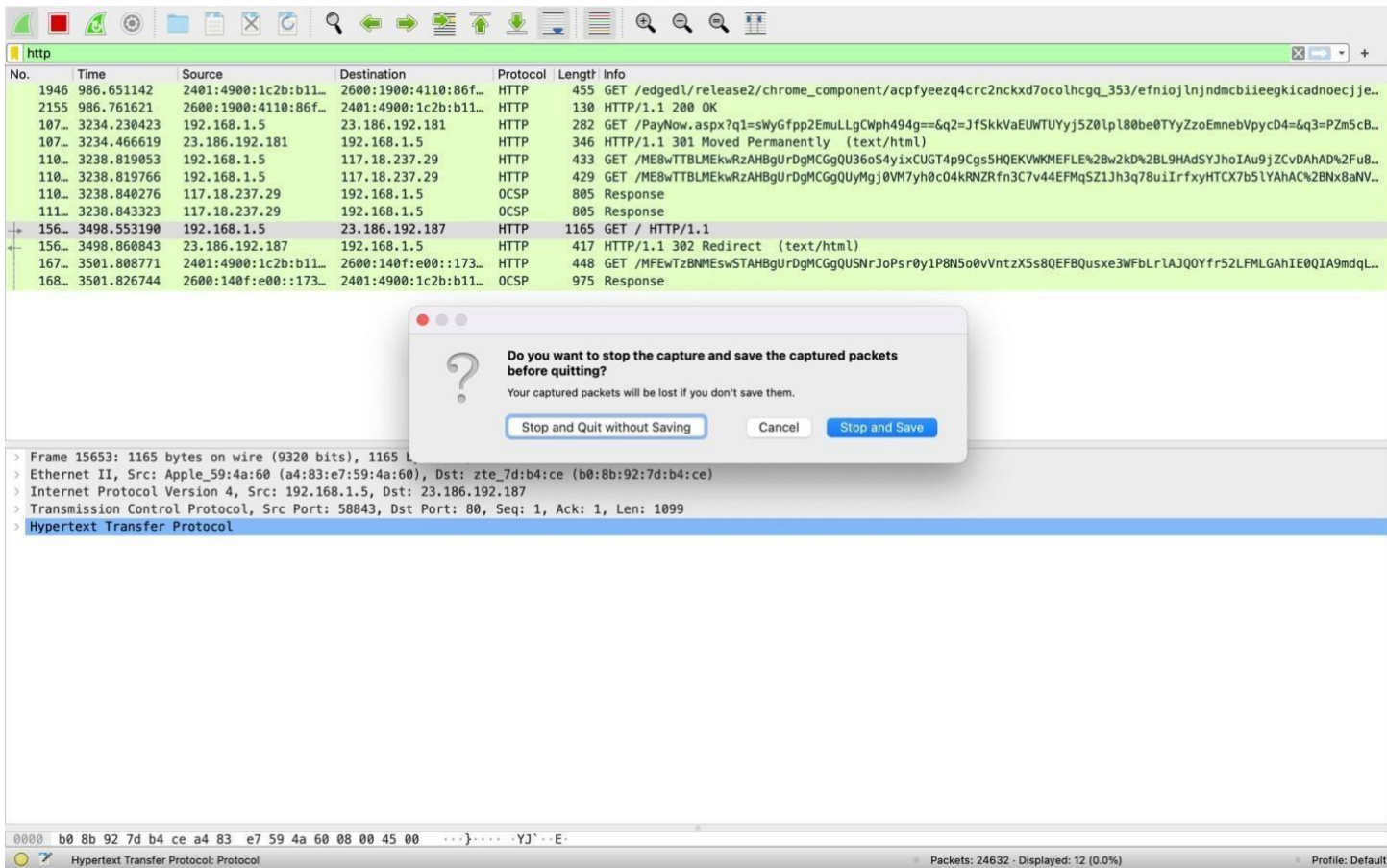
0000 b0 8b 92 7d b4 ce a4 83 e7 59 4a 60 08 00 45 00 ...}....YJ...E-
 Hypertext Transfer Protocol: Protocol Packets: 24543 - Displayed: 12 (0.0%) Profile: Default

> Frame 15653: 1165 bytes on wire (9320 bits), 1165 bytes captured (9320 bits) on interface en0, id 0
 > Ethernet II, Src: Apple_59:4a:60 (a4:83:e7:59:4a:60), Dst: zte_7d:b4:ce (b0:8b:92:7d:b4:ce)
 > Internet Protocol Version 4, Src: 192.168.1.5, Dst: 23.186.192.187
 > Transmission Control Protocol, Src Port: 58843, Dst Port: 80, Seq: 1, Ack: 1, Len: 1099
 > Hypertext Transfer Protocol

0000 b0 8b 92 7d b4 ce a4 83 e7 59 4a 60 08 00 45 00 ...}....YJ...E-
 0010 04 7f 00 00 40 00 40 06 9c 56 c0 a8 01 05 17 ba ...@.@-V...
 0020 c0 bb e5 db 00 50 2d e9 39 38 18 43 08 3d 80 18 ...P- 98 C=-
 0030 08 04 4c 0e 00 00 01 01 08 0a 2d 7f 6d 17 41 8e ...L...-m-A-
 0040 bd 61 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ...aGET / HTTP/1.1
 0050 00 0a 48 6f 73 74 3a 20 77 77 77 2e 63 75 63 68 ...Host: www.cuch
 0060 64 2e 69 6e 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e ...d.in-Co nnection
 0070 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 61 ...: keep-a live- Ca
 0080 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 ...che-Cont rol: max
 0090 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 65 2d ...-age-0 Upgrade-
 00a0 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 ...Insecure -Request
 00b0 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 ...s: 1-Us er-Agent
 00c0 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 4d ...: Mozill a/5.0 (M
 00d0 61 63 69 6e 74 6f 73 68 3b 20 49 6e 74 65 6c 20 ...acintosh ; Intel
 00e0 4d 61 63 20 4f 53 20 58 20 31 30 5f 31 35 5f 37 ...Mac OS X 10_15_7
 00f0 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 ...) AppleWebKit/53
 0100 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b ...7.36 (KH TML, lik
 0110 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f ...e Gecko) Chrome/
 0120 31 30 34 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 ...104.0.0.0 Safari
 0130 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 3a .../537.36 -Accept:
 0140 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 ...text/ht ml,appli
 0150 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c ...cation/x tml+xml
 0160 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c ... ,applic ation/xml
 0170 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 76 69 ...;q=0.9,i mage/avi
 0180 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d 61 ...f, image/ webp, ima
 0190 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e ...ge/apng, */s;q=0.
 01a0 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 69 ...8,applic ation/si
 01b0 67 6e 65 64 2d 65 78 63 68 61 6e 67 65 3b 76 3d ...gned-exc hange;v=

No.: 15653 - Time: 3498.553190 - Source: 192.168.1.5 - Destination: 23.186.192.187 - Protocol: HTTP - Length: 1165 - Info: GET / HTTP/1.1

Help Close



No.	Time	Source	Destination	Protocol	Length	Info
1946	986.651142	2401:4900:1c2b:b11...	2600:1900:4110:86f...	HTTP	455	GET /edgedl/release2/chrome_component/acpfyeezq4crc2nckxd7ocolhcgq_353/efniojlnjndmcbiieegkicadnoecjje...
2155	986.761621	2600:1900:4110:86f...	2401:4900:1c2b:b11...	HTTP	130	HTTP/1.1 200 OK
107...	3234.230423	192.168.1.5	23.186.192.181	HTTP	282	GET /PayNow.aspx?q1=sWyGfpp2EmuLlgCWph494g==6q2=JfSkkVaEUWTUYy5Z0lp180be0TYyZzoEmnebVpycD4=&q3=PZm5cB...
107...	3234.466619	23.186.192.181	192.168.1.5	HTTP	346	HTTP/1.1 301 Moved Permanently (text/html)
110...	3238.819053	192.168.1.5	117.18.237.29	HTTP	433	GET /ME8wTTBLMEkwRzAHBgUrDgMCgQU36o54yixCUGT4p9Cgs5H0EKVWkMEFLE%2Bw2kD%2BL9HAdSYJhoIAu9jZCvDAhAD%2Fu8...
110...	3238.819766	192.168.1.5	117.18.237.29	HTTP	429	GET /ME8wTTBLMEkwRzAHBgUrDgMCgQU36o54yixCUGT4p9Cgs5H0EKVWkMEFLE%2Bw2kD%2BL9HAdSYJhoIAu9jZCvDAhAD%2Fu8...
110...	3238.840276	117.18.237.29	192.168.1.5	OCSP	805	Response
111...	3238.843323	117.18.237.29	192.168.1.5	OCSP	805	Response
156...	3498.553190	192.168.1.5	23.186.192.187	HTTP	1165	GET / HTTP/1.1
156...	3498.860843	23.186.192.187	192.168.1.5	HTTP	417	HTTP/1.1 302 Redirect (text/html)
167...	3501.808771	2401:4900:1c2b:b11...	2600:140f:e00::173...	HTTP	448	GET /MFEwTzBNMEswSTAHBgUrDgMCgQU36o54yixCUGT4p9Cgs5H0EKVWkMEFLE%2Bw2kD%2BL9HAdSYJhoIAu9jZCvDAhAD%2Fu8...
168...	3501.826744	2600:140f:e00::173...	2401:4900:1c2b:b11...	OCSP	975	Response

Do you want to stop the capture and save the captured packets before quitting?
Your captured packets will be lost if you don't save them.

Stop and Quit without Saving Cancel Stop and Save

Frame 15653: 1165 bytes on wire (9320 bits), 1165 bytes captured (9320 bits) on interface 0
Ethernet II, Src: Apple_59:4a:60 (a4:83:e7:59:4a:60), Dst: zte_7d:b4:ce (b0:8b:92:7d:b4:ce)
Internet Protocol Version 4, Src: 192.168.1.5, Dst: 23.186.192.187
Transmission Control Protocol, Src Port: 58843, Dst Port: 80, Seq: 1, Ack: 1, Len: 1099
Hypertext Transfer Protocol

0000 b0 8b 92 7d b4 ce a4 83 e7 59 4a 60 08 00 45 00 ...}....-YJ'--E-
Hypertext Transfer Protocol: Protocol

Packets: 24632 · Displayed: 12 (0.0%) Profile: Default

Learning Outcomes:

Identify requests (from client) and response packets. Find HTTP version, response code/phrase, requested file (including size). Observe single small file (e.g., simple html file) request/response behaviour and the request/response behaviour for a file that has already been received. Observe how a larger file is sent in multiple segments Observe multi-file (e.g., web page with image) request/response behaviour. Observe request/response behaviour for a page that needs authentication.



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

Evaluation Grid (To be created as per the SOP and Assessment guidelines by the faculty):

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1			
2			
3			
4			