Sveučilište u Mostaru

**Fakultet strojarstva, računarstva i elektrotehnike**

**SEMINARSKI RAD**

**Analizatori protokola**

Profesor: dr.sc. Drago Žagar Student: Jozo Skoko

Mostar, prosinac 2018.

Sadržaj

[1 UVOD 1](#_Toc532734169)

[2 ANALIZATOR PROTOKOLA 2](#_Toc532734170)

[2.1 Što je analizator protokola 2](#_Toc532734171)

[2.2 Upotreba analizatora protokola 3](#_Toc532734172)

[3 VRSTE ANALIZATORA PROTOKOLA 5](#_Toc532734173)

[3.1 USB protokol 5](#_Toc532734174)

[3.2 CAN protokol 6](#_Toc532734175)

[3.3 I2C protokol 7](#_Toc532734176)

[3.4 SPI protokol 7](#_Toc532734177)

[3.5 eSPI protokol 8](#_Toc532734178)

[4 SIGURNOST 10](#_Toc532734179)

[4.1 Napadi analizatora protokola 10](#_Toc532734180)

[4.2 Sprječavanje napada 11](#_Toc532734181)

[5 MANE ANALIZATORA PROTOKOLA 12](#_Toc532734182)

[6 WIRESHARK 13](#_Toc532734183)

[7 ZAKLJUČAK 15](#_Toc532734184)

[POPIS SLIKA 16](#_Toc532734185)

[LITERATURA 17](#_Toc532734186)

# 1 UVOD

U složenom svijetu mreža problemi se često događaju. Određivanje točnog uzroka problema u radu složenih sustava je zahtejvno i često može biti jako opasno. U tim slučajevima stručni inženjeri koriste tajno oružje koje se zove analizator protokola. Analizator protokola omogućuje da inžinjer odredi izvor gotovo bilo koje pogreške pod uvjetom da se obrazuje na temeljnom protokolu.

Ovaj seminarski rad predstavit će što je analizator protokola, koji programi se koriste za njegovo korištenje, njegovu konkretnu ulogu, te neke vrste analizatora protokola koje danas imamo.

# 2 ANALIZATOR PROTOKOLA

## 2.1 Što je analizator protokola

Analizator protokola ili "nosač paketa", alat je koji se koristi za presretanje prometa, pohranjivanje i prikazivanje u dekodiranom, čitljivom stanju čovjeku. Suvremeni analizatori protokola kao što je Wireshark mogu čak i otkriti rudimentarne probleme samostalno, a zatim provesti statističke analize sa zarobljenim podacima.

Bez obzira na značajke, analizatori protokola rade na istom osnovnom putu. Oni se umetnu u mrežni stog i kopiraju sav promet u međuspremnik ili datoteku. Većina će također postaviti mrežni upravljački program u "promiskujući način", što u osnovi dopušta tim alatima da preuzimaju sav promet koji ulazi u mrežni stog umjesto da samo prikuplja promet namijenjen samom sustavu. Analizatori protokola dolaze u obliku namjenskih hardvera koji se mogu povezati s ugrađenim uređajem. Međutim, da bi se tumačili podatci koji se dobiju od hardvera, potrebno je korisničko sučelje koje prikazuje podatke sabirnice u obliku koji je čitljiv za ljude. Dakle, ukratko, analizator protokol je kombinacija namjenskih hardvera i softvera koji rade zajedno. Radeći zajedno, hardver bilježi podatke, a softver prikazuje snimljene podatke.

Ali nisu sva sučelja ista. Neki samo prikazuju snimanje podataka, dok drugi omogućuju pretraživanje, definiranje filtara, prepoznavanje uzoraka i dekodiranje, u stvarnom vremenu.[1]



Slika 2.1: Izgled analizatora protokola(TPI4000)[2]

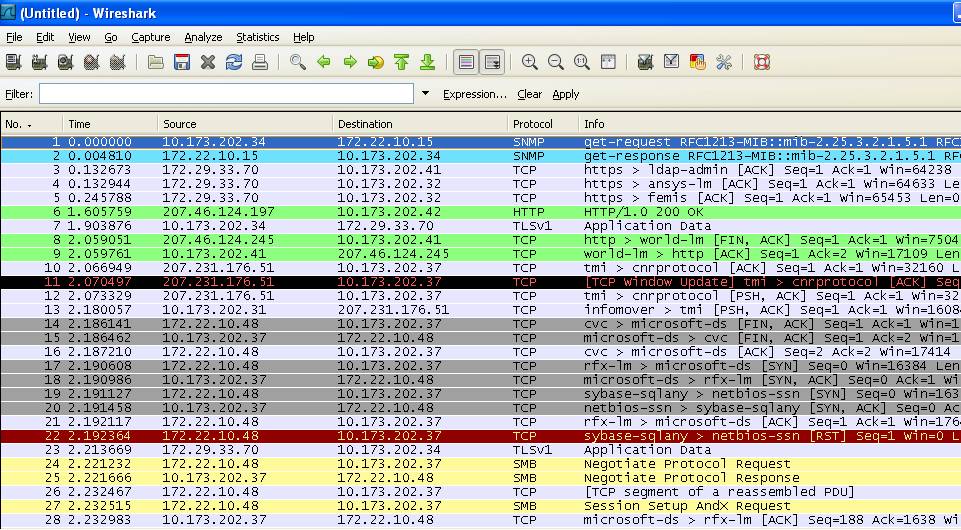
## 2.2 Upotreba analizatora protokola

Upravitelj mreže mora biti pažljiv za analizu i zaštitu mrežnog prometa od prijetnji i slabih performansi. Upravitelji često trebaju otkloniti poteškoće s mrežom kako bi osigurali učinkovito i brzo okruženje mrežnog prometa.

Analizator protokola prikazuje cjelokupan status svih mrežnih aktivnosti pružajući potpunu sliku širine pojasa i korištenja resursa. Ako resurs koristi preveliku širinu pojasa, upravitelj mreže može osloboditi resurs prekidanjem postupka. Međutim, novo primijenjene aplikacije i čvorovi mreže mogu imati neke konfiguracije i probleme s radom, no one se mogu riješiti za nekoliko sekundi pomoću analizatora protokola. Svako djelovanje analizatora protokola izvodi se u stvarnom vremenu.[3]

Ključne funkcije i upotrebe analizatora protokola uključuju:

* Analizirajući mrežna pitanja i probleme
* Praćenje sigurnosti mreže otkrivanjem neovlaštenih pokušaja hakiranja mreže
* Izoliranje elemenata koji uzrokuju štetu
* Praćenje ukupne propusnosti WAN-a (i pojedinačne potrošnje korisnika)
* Generiranje cjelovitog izvješća o mrežnim statistikama organiziranim u tabličnom obliku, grafičkim grafikonima ili kao izravni podaci
* Praćenje podataka koji se prenose ili su u pokretu
* Praćenje ukupnih WAN/LAN i korisničkih/krajnjih točaka sigurnosnih problema i statusa
* Filtriranje neželjenih sadržaja i sprječavanje neovlaštenog pristupa
* Izvođenje operacija otklanjanja pogrešaka na strani klijenta/poslužitelja zbog pogrešaka/problema s komunikacijom
* Praćenje konfiguracije proxy poslužitelja, status vatrozida i konfiguracija, zaštita od neželjenih poruka i ostali sigurnosni aspekti
* Posluživanje kao primarni izvor podataka za praćenje i upravljanje svakodnevnim mrežama
* Reverse inženjerski vlasnički protokoli preko mreže



Slika 2.2: Upravljanje analizatorom protokola - softverski prikaz(Whireshark)[4]

# 3 VRSTE ANALIZATORA PROTOKOLA

IP sniffing i MAC sniffing su neki od najčešćih načina za analizu i ispitivanje prometa koji teče kroz mrežu. I IP i MAC njuškanje oslanjaju se na korištenje mrežne kartice za njuškanje paketa podataka koji odgovaraju određenoj IP ili MAC adresi. Tako administrator mreže lako može analizirati informacijske pakete za otkrivanje svih nedostataka unutar mreže.

Dok Analizatori protokola imaju legitimne koristi u praćenju i rješavanju problema mreže, oni su također naširoko koriste od hakera za dobivanje neovlaštenog pristupa mreži i krađe informacija. Zato je vrlo važno da mrežni menadžeri stavljaju sigurnosne mjere, poput vatrozida, kako bi spriječili prodor u mrežu.

Analizator protokola obuhvaća i analizira signale i podatkovni promet preko komunikacijskog kanala (a ne mreže). Komunikacijski kanal može se razlikovati od komunikacije na brodu do satelitske veze.[5]

## 3.1 USB protokol

USB protokol je daleko najčešći komunikacijski protokol na tržištu potrošača danas. Svatko tko ima računalo, mobitel ili tabletno računalo upotrebljava USB protokol svjesno ili nesvjesno u obliku flash pogona, podatkovnih kartica, USB kabela, punjača itd.

USB označava Universal Serial Bus. Kao što ime sugerira, USB protokol se koristi za prijenos podataka serijski s jednim bitom za drugim. USB je u osnovi anketirana autobusna stanica gdje svi prijenos podataka pokreću domaćini.



Slika 3.1: USB analizator protokola[6]

## 3.2 CAN protokol

Protokol za CAN (Computer Area Network) koristi se za olakšavanje komunikacije između mikrokontrolera i pridruženih uređaja u ugrađenom okruženju. To je osobito korisno u scenarijima gdje računalo nije prisutno.



Slika 3.2: CAN analizator protokola[7]

## 3.3 I2C protokol

I2C protokol koristi se više od četiri desetljeća, pa čak i danas, te uživa značajnu popularnost. I2C, koji je također poznat kao I2C ILI IIC označava Inter-integrirani krug. Pomoću I2C možete uspostaviti komunikaciju kratkog spoja unutar dva IC-a koji se nalaze na istoj ploči.

Jedinstveni prodajni prijedlog I2C protokola leži u jednostavnom dizajnu, prilagodljivim značajkama, vrhunskom rješavanju čipova i robusnom mehanizmu rukovanja pogreškama. Ipak, I2C je također pogođen s nedostacima kao što su spor prijenos stope i iznos nekretnina koje je potrebno na pločici.



Slika 3.3: I2C analizator protokola[8]

## 3.4 SPI protokol

Slično kao i I2C, SPI (Serial Peripheral Interface) također se koristi za komunikaciju kratkog dometa u ugrađenim sustavima. To je serijski komunikacijski protokol koji djeluje u full duplex modu uz pomoć master-slave arhitekture. Može se spojiti više robnih uređaja putem SPI protokola. Međutim SPI podržava samo jedan glavni uređaj.



Slika 3.4: SPI analizator protokola[9]

## 3.5 eSPI protokol

ESPI protokol može se dijeliti s SPI uređajima za spremanje igala ili se odvojiti od SPI sabirnice kako bi se omogućilo bolje performanse, posebno kada eSPI uređaji trebaju koristiti SPI flash uređaje.

Ovaj standard definira signal upozorenja koji koristi eSPI slave da bi zatražio uslugu od glavnog računala. U izvedbenom dizajnu ili dizajnu sa samo jednim eSPI protokolom, svaki eSPI slave će imati svoj alarmni PIN povezan na Alert PIN na eSPI masteru koji je posvećen svakom dijelu, omogućujući eSPI masteru da dade nisku latenciju uslugu jer će eSPI majstor znati koji eSPI dio treba servisirati. U proračunskom dizajnu s više od jednog eSPI robusa, svi upozoreni pribori robovi povezani su s jednim Alert pinom na eSPI masteru u žičanom OR priključku, što će zahtijevati od strane mastera da pregleda sve robove kako bi odredio koje one trebaju uslugu kada je signal upozorenja zaustavljen nizak od jedne ili više perifernih uređaja koji trebaju uslugu. Tek nakon što se svi uređaji servisiraju, signal upozorenja se može povući visoko, jer nijedan eSPI rob na kojem je potreban servis nema signal upozorenja nizak.

Ovaj standard omogućuje dizajnerima korištenje 1-bitne, 2-bitne ili 4-bitne komunikacije pri brzinama od 20 do 66 MHz kako bi dodatno dopustio dizajnerima da sklope performanse i troškove.[10]



Slika 3.5: eSPI analizator protokola[11]

# 4 SIGURNOST

Softver paketnog analizatora često uključuje alate za otkrivanje pokušaja upada i skrivenih mreža. Osim ugrađenih uslužnih programa, postoje mnoge komercijalno dostupne tehnologije dizajnirane za otkrivanje zlonamjernih analizatora protokola. Ovi alati obično rade praćenjem mrežnog prometa i skeniranjem mrežnih kartica u promiskuitetnom načinu rada. Postoji bezbroj dostupnih programa koji to čine, tako da sigurnosni timovi moraju odrediti najbolji softver za svoje potrebe.

## 4.1 Napadi analizatora protokola

Nažalost, mogućnosti analizatora protokola čini ih popularnim alatom za zlonamjerne napade. Napadi protokol analizatora obično uključuju zlonamjerne sudionike koji koriste njuškanje mreže u promiskuitetnom načinu rada. Njuškalo u promiskujalnom načinu sposobno je čitati sve podatke koji teče u/iz pristupne točke na mreži. Napadači zlostavljaju putanje paketa kako bi ukrali podatke, špijunirali mrežni promet i prikupljali informacije kako bi utjecali na buduće napade na mrežu. Analizator protokolskih napada obično cilja korisničke prijave, financijske informacije i poruke e-pošte. Povezivanje s nesigurnim mrežama kao što su javni ili besplatni Wi-Fi korisnicima povećava rizik za napade paketa analizatora jer ih napadači lakše njuškaju.

Uz jednostavno njušenje podataka, napadački su čimbenici često upotrebljavali analizatore protokola kako bi izvršili sofisticirane napade. Ti napadi mogu uključivati (ali nisu ograničeni na):

* Napadi napadanja: Paketni analizatori mogu se koristiti za prikupljanje informacija o korisnicima i uređajima koji su povezani s mrežom koju napadač namjerava prevariti.
* Slaganje sesije: U ovoj vrsti napada, sniferi paketa koriste se za krađu kolačića sesije kako bi se lažno predstavljali kao drugi korisnici.
* Man-in-the-middle napad: Napadači mogu koristiti mrežne analizatore za presretanje poruka između dviju stranaka i potom krivotvoriti poruke od stranke do zabave.

## 4.2 Sprječavanje napada

Postoji nekoliko koraka koje bi sva poduzeća trebala poduzeti kako bi osigurala da su zaštićeni od napada koji koriste analizatore protokola. Za početak, sigurne protokole trebaju se koristiti kad god je to moguće kako bi se osiguralo da su podaci kriptirani prije slanja preko mreže. Primjeri sigurnih protokola uključuju HTTPS, Secure File Transfer Protocol (SFTP) i Secure Shell (SSH). Ako se mora upotrebljavati nesigurni protokol, organizacija i dalje može zaštititi svoju mrežu od napada nosača paketa pomoću softvera za šifriranje prije prijenosa podataka.

Osim upotrebe sigurnih protokola i šifriranja podataka, organizacije trebaju optimizirati mrežnu strukturu kako bi se zaštitile od napada koji koriste analizatore mreže. Preporuča se da mreže budu izgrađene tehnologijom prekidača (a ne hub tehnologije) kad god je to moguće. Nakon primitka poruke, prekidač će prenijeti tu poruku samo do njegovog namjeravanog primatelja, dok hub prenosi poruke koje primi na cijeloj mreži. Ova značajka čini preklopnike inherentno sigurnijim od čvorišta, osobito za sprečavanje napada analizatora paketa.

Još jedna jaka opcija za sprječavanje napada nosača paketa je korištenje tehnologije daljinskog računanja kako bi se osiguralo da su svi podaci kriptirani prije slanja preko mreže. Ova je metoda posebno učinkovita u sprečavanju bežičnih snipera. VPN (Virtual Private Network), VNC (Virtual Network Computing) i RDP (Remote Desktop Protocol) zajednički su primjeri programa koji pružaju šifrirano daljinsko upravljanje. Korištenje udaljenog računalnog programa u kombinaciji s gore opisanim metodama povećat će sigurnost mreže dodavanjem višestrukih slojeva enkripcije.

Naposljetku, organizacija koja se želi zaštititi od napada protokolskih analizatora redovito treba njuškati vlastite mreže koristeći bežični softver za njuškanje. Na taj način organizacija može pregledati svoju mrežu iz napadačke perspektive kako bi otkrila ranjivosti na snižavanje napada i napade u tijeku.[12]

# 5 MANE ANALIZATORA PROTOKOLA

Čest problem koji se pojavljuje s analizatorima protokola je nemogućnost preciznog prepoznavanja - a time i dekodiranja - protokola koji se pokreće preko ne-predefiniranog broja porta. U današnjem sigurnosnom svjesnom računalnom svijetu, dobro poznate aplikacije na ne tako poznatim lukama su zajednička obrana od zlonamjernih hakera. Neki dekoderi prepoznaju promet bez obzira na luku na kojoj radi, dok drugi ne definiraju protokol samo njegovim nižim slojem (tj. TCP ili UDP), što također znači da dekoder ne daje korisnije polje za specifične podatke dekodiranja. Neki analizatori omogućuju modificiranje dekodera da prepozna više od zadane priključnice za određene protokole.

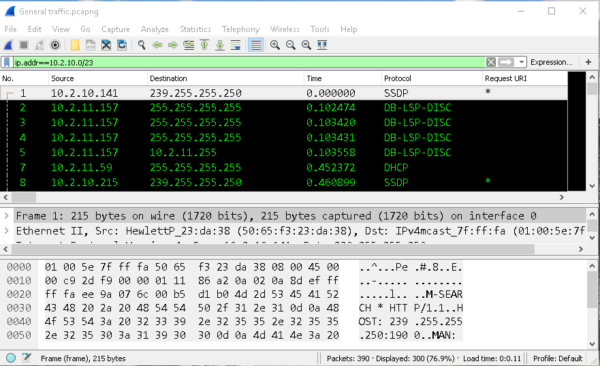
Prodavači protokola-analizatora često se hvale zbog sposobnosti stručnjaka za analizu svojih proizvoda, pri čemu analizator čita paket ili niz paketa i izvještava korisne informacije o zarobljenim paketima. Stručna analiza može prijaviti anomalije prometa ili zlonamjerne pakete ili potpuno dekodirati seriju tokova podataka između dva domaćina. Opcija dekodiranja je neprocjenjiva jer možete vidjeti cijeli komunikacijski tok podataka jednostavno klikom na paket. Na primjer, možete kliknuti HTTP paket i vidjeti web stranicu koju predstavlja kao krajnji korisnik koji bi je mogao vidjeti kada se izvede temeljni HTML kod. Ostale uobičajene značajke uključuju filtriranje prije i poslije snimanja (mogućnost pronalaženja određenih paketa koji zadovoljavaju određene kriterije), aktivira (pokretanje sekundarne radnje kada se dogodi unaprijed definirani paketni uzorak), ponavljanje (mogućnost reprodukcije zabilježenih paketa preko mreža), statistike prometa, izvješćivanje i upravljanje višestrukim senzorima s jedne konzole.[13]

# 6 WIRESHARK

Wireshark je najistaknutiji i najčešće korišten softvare za analizator mrežnog protokola na svijetu. Omogućuje uvid u događaje u mreži na mikroskopskoj razini i to je 'de facto' (i često 'de jure') standard u mnogim komercijalnim i neprofitnim tvrtkama, vladinim agencijama i obrazovnim ustanovama. Wireshark razvoj uspijeva zahvaljujući volonterskim doprinosima mrežnih stručnjaka diljem svijeta i nastavak je projekta koji je započeo Gerald Combs 1998.

Mogućnosti koje nudi Wireshark[14]:

* Duboki pregled stotina protokola
* Analiza snimanja uživo i izvanmrežno
* Standardni paketni preglednik s tri okna
* Multi-platforma: radi na Windows, Linux, MacOS, Solaris, FreeBSD, NetBSD, i mnogi drugi
* Prikupljene mrežne podatke može se pregledavati putem GUI-ja ili pomoću TShark uslužnog programa TTY-mode
* Najmoćniji filtri za prikaz u industriji
* Bogata VoIP analiza
* Čitanje/pisanje mnogih različitih formata datoteka za snimanje: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (komprimirani i nekomprimirani), Sniffer® Pro i NetXray®, Network Instruments Observer , NetScreen snoop, Novell LANalyzer, RADCOM WAN / LAN analizator, Shomiti / Finisar Surveyor, Tektronix K12xx, vizualne mreže Visual UpTime, WildPackets EtherPeek / TokenPeek / AiroPeek i mnogi drugi
* Snimanje datoteka sa stisnutim gzipom može se dekomprimirati u letu
* Podaci uživo mogu se pročitati iz Ethernet, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI i drugi (ovisno o vašoj platformi)
* Potpora za dešifriranje za mnoge protokole, uključujući IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP i WPA / WPA2
* Pravila bojanja mogu se primijeniti na paketni popis za brzu, intuitivnu analizu
* Izlaz se može izvesti u XML, PostScript®, CSV ili običan tekst



Slika 6.1: FIltriranje IP adresa u Wireshark-u[15]

# 7 ZAKLJUČAK

Na temelju informacija prikupljenih u radu vidimo da analizator protokola ima bitnu ulogu u mrežnom sustavu. Svako ozbiljno poduzeće, pogotovo ona koja se bave čuvanjem izradom aplikacija koje koriste velik broj korisnika ili općenito čuvanjem podataka raznih korisnika trebaju implementirati u svoj poslovni sustav korištenje analizatora protokola zbog sigurnosti. Postoje više vrsta analizatora protokola stoga svako poduzeće može naći sebi odgovarajući za svoje potrebe. Zbog česte nemoralne potrebe ljudi za njušenjem i krađom tuđih podataka potrebno je imati stručno obučene inžinjere koji su ovladali upotrebom analizatora protokola kako bi zaštitili podatke od budućih pokušaja napada na podatke u čemu će im pomoći softveri sa prilagođenim sučeljem koji upravljaju hardverskim dijelom analizatora protokola.

# POPIS SLIKA

[Slika 2.1: Izgled analizatora protokola 2](#_Toc524705378)

[Slika 2.2: Upravljanje analizatorom protokola - softverski prikaz(Whireshark) 4](#_Toc524705379)

[Slika 3.1: USB analizator protokola 6](#_Toc524705380)

[Slika 3.2: CAN analizator protokola 6](#_Toc524705381)

[Slika 3.3: I2C analizator protokola 7](#_Toc524705382)

[Slika 3.4: SPI analizator protokola 8](#_Toc524705383)

[Slika 3.5: eSPI analizator protokola 9](#_Toc524705384)

[Slika 6.1: FIltriranje IP adresa u Wireshark-u 14](#_Toc524705385)

# LITERATURA

[1] Arstechnica, “The power fo protocol analyzer.” .

[2] “TPI4000.” [Online]. Available: http://www.ferret.com.au/c/tekmark-australia/new-tektronix-tpi4000-protocol-analysers-allow-users-to-test-multiple-serial-protocols-on-a-single-instrument-n1828556.

[3] Techopedia, “Packet analayzer.” [Online]. Available: https://www.techopedia.com/definition/25323/packet-analyzer%0D.

[4] “Wireshark IP’s.” [Online]. Available: https://seclists.org/wireshark/2009/Oct/att-466/image001.jpg .

[5] Totalphase, “What is packet sniffer.” [Online]. Available: https://www.totalphase.com/blog/2017/07/what-is-a-packet-sniffer/.

[6] “Beagle usb 5000.” [Online]. Available: https://www.totalphase.com/products/beagle-usb5000-v2-usb2/.

[7] “Komodo.” [Online]. Available: https://www.totalphase.com/products/komodo-canduo/.

[8] “Beagle 12.” [Online]. Available: https://www.totalphase.com/products/beagle-i2cspi/.

[9] “SPI.” [Online]. Available: https://www.tme.eu/gb/details/tp240141/development-kits-others/total-phase/aardvark-i2cspi-host-adapter/.

[10] Totalphase, “What is protocol analayzer.” [Online]. Available: https://www.totalphase.com/blog/2017/06/what-is-a-protocol-analyzer/.

[11] “eSPI.”

[12] Veracode, “Packet analayzer security.” [Online]. Available: https://www.veracode.com/security/packet-analyzer.

[13] I. Protoday, “Common problems.” [Online]. Available: https://www.itprotoday.com/compute-engines/6-network-protocol-analyzers.

[14] Wireshark, “Wireshark.”

[15] “Wireshark picture.” [Online]. Available: https://networksecuritytools.com/how-to-filter-ip-address-using-wireshark/%0D.