

K
U
L
A
N
I
M

K
I
L
A
V
U
Z
U





T.C

FIRAT ÜNİVERSİTESİ
TEKNOLOJİ FAKÜLTESİ
ADLİ BİLİŞİM MÜHENDİSLİĞİ BÖLÜMÜ

ADLİ BİLİŞİM İNCELEME YAZILIMLARI DERSİ
Wireshark KULLANIM KILAVUZU

Hazırlayan: FUNDA YÜKSEL
(190509022)

Öğretim Görevlisi: Doç. Dr. Şengül DOĞAN

OCAK-2022

İÇİNDEKİLER

1. Wireshark Nedir?	4
1.1 Ağ Analizi ve Kullanım Alanları	7
2. Wireshark Kurulumu	8
2.1 Windows İşletim Sistemine Yükleme	8
2.2 Linux İşletim Sistemine Yükleme	14
3.Kullanıcı Arayüz Sekmeleri	14
3.1 “Ana” Araç Çubuğu	14
3.2 “Filtre” Araç Çubuğu	15
3.3 “Paket Listesi” Bölmesi	20
3.4 “Paket Ayrıntıları” Bölmesi	21
3.5 “Paket Baytları” Bölmesi	22
3.6 Durum Çubuğu	23
3.7 Açılır Menüler	23
3.8 Dosya Menüsü	28
3.9 Düzenle Menüsü	30
3.10 Görünüm Menüsü	31
3.11 Git Menüsü	34
3.12 Yakala Menüsü	35
3.13 Analiz Menüsü	36
3.14 İstatistikler Menüsü	38
3.15 Telefon Menüsü	50
3.16 Kablosuz Menüsü	55
3.17 Araçlar Menüsü	56
3.18 Yardım Menüsü	57

1. WIRESHARK NEDİR?

Wireshark, 1998 yılında Ethereal adıyla faaliyete başlayan bir projedir. Ağ uzmanlarının katkılarıyla bu program günden güne gelişerek önde gelen ağ protokol analizcisi haline gelmiştir. Wireshark ismiyle çıkan bu yazılım, bilgisayara ulaşan paketleri yakalamaya ve bu paketlerin içeriğini görüntülemeye imkân tanır. Başka bir deyişle, bilgisayara bağlı olan her türlü ağ kartlarındaki (Ethernet kartı veya modem kartları) tüm TCP/IP mesajlarını analiz edebilen bir programdır. Wireshark, günümüzde çok amaçlı kullanılır. Şebeke problemlerinde sorun çözmek, güvenlik problemlerini sınamak, uygulamaya konulan protokollerde oluşan hataları onarmak veya arındırmak, ağ protokolünün içerisindeki bilgileri öğrenebilmek için Wireshark programı kullanılır.

Wireshark aracının özellikleri:

- Kullanıcı dostudur.
- Ücretsiz kullanılabilir.
- Çoklu işletim sistemi desteği sağlaması: Windows, Linux, MacOS
- Birçok kritere göre paket filtreleme desteği sağlar.
- Yakalanan paketlerin çeşitli formatlarda kayıt eder.
- Çeşitli istatistikler oluşturur.
- Anlık olarak paket yakalayıp görüntüleyebilme özellikleri bulunmaktadır.
- Geniş protokol desteğine sahiptir.
- Desteklenen protokoller şunlardır:

3COMXNS, 3GPP2 A11, 802.11 MGT, 802.11 Radiotap, 802.3 Slow protocols, 9P, AAL1, AAL3/4, AARP, ACAP, ACN, ACSE, ACtrace, ADP, AFP, AFS (RX), AgentX, AH, AIM, AIM Administration, AIM Advertisements, AIM BOS, AIM Buddylist, AIM Chat, AIM ChatNav, AIM Directory, AIM E-mail, AIM Generic, AIM ICQ, AIM Invitation, AIM Location, AIM Messaging, AIM OFT, AIM Popup, AIM Signon, AIM SSI, AIM SST, AIM Stats, AIM Translate, AIM User Lookup, AJP13, ALC, ALCAP, AMR, ANS, ANSI BSMAP, ANSI DTAP, ANSI IS-637-A Teleservice, ANSI IS-637-A Transport, ANSI IS-683-A (OTA (Mobile)), ANSI IS-801 (Location Services (PLD)), ANSI MAP, AODV, AOE, ARCNET, Armagetronad, ARP/RARP, ARTNET, ASAP, ASF, ASN1, ASP, ATM, ATM LANE, ATP, ATSVC, Auto-RP, AVS WLANCAP, AX4000, BACapp, BACnet, Basic Format XID, BEEP, BER, BFD Control, BGP, BICC, BitTorrent, Boardwalk, BOFL, BOOTP/DHCP, BOOTPARAMS, BOSSVR, BROWSER, BSSAP, BSSGP, BUDB, BUTC, BVLC, CAMEL, CAST, CBAPDev, CCSDS, CCSRL, CDP, CDS_CLERK, cds_solicit, CDT, CFLOW, CGMP, CHDLC, CIGI, CIMD, CIP, CISCOWLL2, CLDAP, CLEARCASE, CLNP, CLTP, CMIP, CMP, CMS, CONV, COPS, COSEVENTCOMM, CoSine, COSNAMING, COTP, CPFI, CPHA, cprpc_server, CRMF, CSM_ENCAPS, CUPS, DAAP, DAP, Data, dc, DCCP, DCE_DFS, dce_update, DCERPC, DCOM, DCP, DDP, DDTP, DEC_DNA, DEC_STP, DFS, DHCPFO, DHCPv6, DIAMETER, dicom, DIS, DISP, DISTCC, DLSw, DLT User A, DLT User B, DLT User C, DLT User D, DNP 3.0, DNS, DNSSERVER, DOCSIS, DOCSIS BPKM-ATTR,

DOCSIS BPKM-REQ, DOCSIS BPKM-RSP, DOCSIS DSA-ACK, DOCSIS DSAREQ, DOCSIS DSA-RSP, DOCSIS DSC-ACK, DOCSIS DSC-REQ, DOCSIS DSC-RSP, DOCSIS DSD-REQ, DOCSIS DSD-RSP, DOCSIS INT-RNG-REQ, DOCSIS MAC MGMT, DOCSIS MAP, DOCSIS REGACK, DOCSIS REG-REQ, DOCSIS REG-RSP, DOCSIS RNG-REQ, DOCSIS RNG-RSP, DOCSIS TLVs, DOCSIS type29ucd, DOCSIS UCCREQ, DOCSIS UCC-RSP, DOCSIS UCD, DOCSIS VSIF, DOP, DRSUAPI, DSI, DSP, DSSETUP, DTP, DTSPROVIDER, DTSSTIME_REQ, DUA, DVMRP, E.164, EAP, EAPOL, ECHO, EDONKEY, EDP, EFS, EIGRP, ENC, ENIP, ENRP, ENTTEC, EPM, EPMv4, ESIS, ESP, ESS, ETHERIC, ETHERIP, Ethernet, EVENTLOG, FC, FC ELS, FC FZS, FC-dNS, FC-FCS, FC-SB3, FC-SP, FC-SWILS, FC_CT, FCIP, FCP, FDDI, FIX, FLDB, FR, Frame, FRSAPI, FRSRPC, FTAM, FTBP, FTP, FTP-DATA, FTSERVER, FW-1, G.723, GIF image, giFT, GIOP, GMRP, GNM, GNUTELLA, GPRS NS, GPRS-LLC, GRE, Gryphon, GSM BSSMAP, GSM DTAP, GSM RP, GSM SMS, GSM SMS UD, GSM_MAP, GSM_SS, GSS-API, GTP, GVRP, H.223, H.225.0, H.235, H.245, H.261, H.263, H.263 data, H1, h221nonstd, H248, h450, HCLNFSD, HPEXT, HPSW, HSRP, HTTP, HyperSCSI, IAP, IAPP, IAX2, IB, ICAP, ICBAAccoCB, ICBAAccoCB2, ICBAAccoMgt, ICBAAccoMgt2, ICBAAccoServ, ICBAAccoServ2, ICBAAccoServSRT, ICBAAccoSync, ICBABrowse, ICBABrowse2, ICBAGErr, ICBAGErrEvent, ICBALDev, ICBALDev2, ICBAPDev, ICBAPDev2, ICBAPDevPC, ICBAPDevPCEvent, ICBAPersist, ICBAPersist2, ICBARTAuto, ICBARTAuto2, ICBASState, ICBASStateEvent, ICBASysProp, ICBATime, ICEP, ICL_RPC, ICMP, ICMPv6, ICP, ICQ, IDispatch, IDP, IEEE 802.11, IEEE802a, iFCP, IGAP, IGMP, IGRP, ILMI, IMAP, INAP, INITSHUTDOWN, IOXIDResolver, IP, IP/IEEE1394, IPComp, IPDC, IPFC, IPMI, IPP, IPv6, IPVS, IPX, IPX MSG, IPX RIP, IPX SAP, IPX WAN, IRC, IrCOMM, IRemUnknown, IRemUnknown2, IrLAP, IrLMP, ISAKMP, iSCSI, ISDN, ISIS, ISL, ISMP, iSNS, ISUP, isup_thin, ISystemActivator, itunes, IUA, IuUP, Jabber, JFIF (JPEG) image, Juniper, JXTA, JXTA Framing, JXTA Message, JXTA UDP, JXTA Welcome, K12xx, KADM5, KINK, KLM, Kpasswd, KRB4, KRB5, KRB5RPC, L2TP, LANMAN, LAPB, LAPBETHER, LAPD, Laplink, LDAP, LDP, Line-based text data, LLAP, llb, LLC, LLDP, LMI, LMP, Log, LogotypeCertExtn, LOOP, LPD, LSA, Lucent/Ascend, LWAPP, LWAPP-CNTL, LWAPP-L3, LWRES, M2PA, M2TP, M2UA, M3UA, MACC, Malformed packet, Manolito, MAP_DialoguePDU, MAPI, MDS Header, Media, MEGACO, message/http, Messenger, MGCP, MGMT, MIME multipart, MIPv6, MMS, MMSE, Mobile IP, Modbus/TCP, MOUNT, MPEG1, MPLS, MPLS Echo, MQ, MQ PCF, MRDISC, MS NLB, MS Proxy, MSDP, MSMMS, MSNIP, MSNMS, MSRP, MTP2, MTP3, MTP3MG, MySQL, NBAP, NBDS, NBIPX, NBNS, NBP, NBSS, NCP, NCS, NDMP, NDPS, NetBIOS, Netsync, nettl, NFS, NFSACL, NFSAUTH, NHRP, NIS+, NIS+ CB, NJACK, NLM, NLSP, NMAS, NMPI, NNTP, NORM, NS_CERT_EXTS, NSIP, NSPI, NTLMSSP, NTP, Null, NW_SERIAL, OAM AAL, OSCP, OLSR, OPSI, OSPF, P_MUL, PAGP, PAP, PARLAY, PCLI, PCNFSD, PER, PFLOG, PFLOG-OLD, PGM, PGSQL, PIM, PKCS-1, PKInit, PKIX Certificate, PKIX1EXPLICIT, PKIX1IMPLICIT, PKIXPROXY, PKIXQUALIFIED, PKIXTSP, PKTC, PNDPCP, PN-RT, PNIO, PNP, POP, Portmap, PPP, PPP BACP, PPP BAP, PPP CBCP, PPP CCP, PPP CDPCP, PPP CHAP, PPP Comp, PPP IPCP, PPP IPV6CP, PPP

LCP, PPP MP, PPP MPLSCP, PPP OSICP, PPP PAP, PPP PPPMux, PPP PPPMuxCP, PPP VJ, PPP-HDLC, PPPoED, PPPoES, PPTP, PRES, Prism, PTP, PVFS, Q.2931, Q.931, Q.933, QLLC, QUAKE, QUAKE2, QUAKE3, QUAKEWORLD, R-STP, RADIUS, RANAP, Raw, Raw_SigComp, Raw_SIP, rdaclif, RDM, RDT, Redback, REMACT, REP_PROC, RIP, RIPng, RLM, Rlogin, RMCP, RMI, RMP, RNSAP, ROS, roverride, RPC, RPC_BROWSER, RPC_NETLOGON, RPL, rpriv, RQUOTA, RRAS, RS_ACCT, RS_ATTR, rs_attr_schema, RS_BIND, rs_misc, RS_PGO, RS_PLCY, rs_prop_acct, rs_prop_acl, rs_prop_attr, rs_prop_pgo, rs_prop_plcy, rs_pwd_mgmt, RS_REPADM, RS_REPLIST, rs_repmgr, RS_UNIX, rsec_login, RSH, rss, RSTAT, RSVP, RSYNC, RTcfg, RTCP, RTmac, RTMP, RTP, RTP Event, RTPS, RTSE, RTSP, RUDP, RWALL, RX, SADMIND, SAMR, SAP, SCCP, SCCPMG, SCSI, SCTP, SDLC, SDP, SEBEK, SECIDMAP, Serialization, SES, sFlow, SGI MOUNT, Short frame, SIGCOMP, SIP, SIPFRAG, SIR, SKINNY, SLARP, SliMP3, SLL, SM, SMB, SMB Mailslot, SMB Pipe, SMB2, SMB_NETLOGON, smil, SMPP, SMRSE, SMTP, SMUX, SNA, SNA XID, SNAETH, Sndcp, SNMP, Socks, SONMP, SoulSeek, SPNEGO, SPNEGO-KRB5, SPOOLSS, SPP, SPRAY, SPX, SRP, SRVLOC, SRVSVC, SSCF-NNI, SSCOP, SSH, SSL, SSS, STANAG 4406, STANAG 5066, STAT, STAT-CB, STP, STUN, SUA, SVCCTL, Symantec, Synergy, Syslog, T.38, TACACS, TACACS+, TALI, TANGO, TAPI, TCAP, TCP, TDMA, TDS, TEL_MANAGEMENT, TELNET, Teredo, TFTP, TIME, TIPC, TKN4Int, TNS, Token- Ring, TPCP, TPKT, TR MAC, TRKSVR, TSP, TTP, TUXEDO, TZSP, UBIKDISK, UBIKVOTE, UCP, UDP, UDPENCAP, UDPlite, UMA, Unreassembled fragmented packet, V.120, V5UA, Vines ARP, Vines Echo, Vines FRP, Vines ICP, Vines IP, Vines IPC, Vines LLC, Vines RTP, Vines SPP, VLAN, VNC, VRRP, VTP, WAP SIR, WBXML, WCCP, WCP, WHDLC, WHO, WINREG, WINS-Replication, WKSSVC, WLANCERTXTN, WSP, WTLS, WTP, X.25, X.29, X11, X411, X420, X509AF, X509CE, X509IF, X509SAT, XDMCP, XML, XOT, XYPLEX, YHOO, YMSG, YPBIND, YPPASSWD, YPSERV, YPXFRZEBRA, ZIP

- Birçok farklı tipte yerel ağ medya trafiği Wireshark tarafından yakalanabilir. Hangi medya tiplerinin desteklendiği, kullanılan işletim sistemi dâhil birçok bilgi Wireshark tarafından tespit edilebilir.
- Wireshark, diğer paket yakalama programlarına göre, yakaladığı paketlerin büyük bir kısmını açabilir.
- Birçok protokol için şifre çözme desteği sunar. Örneğin;
 - IPsec, Internet Protocol Security (İnternet Güvenlik Protokolü)
 - ISAKMP, Internet Security Association and Key Management Protocol (İnternet Bağ ve Şifre Yönetim Protokolü)
 - Kerberos
 - SNMPv3, Simple Network Management Protocol Version 3 (Basit Ağ Yönetim Protokolü Sürüm 3)
 - SSL, Secure Sockets Layer (Emniyetli Yuva Katmanı)
 - TLS, Transport Layer Security (Taşıma Katmanı Güvenliği)
 - WEP, Wired Equivalent Privacy (Kabloya Eşdeğer Mahremiyet)

- WPA, Wi-Fi Protected Access (Wi-Fi Korumalı Erişim)
- WPA2, Wi-Fi Protected Access 2 (Wi-Fi Korumalı Erişim 2)

Wireshark, açık bir kaynak yazılım projesidir ve GPL, General Public License (Genel Kamu Lisansı), altında bırakılır. Serbest bir şekilde, her türlü bilgisayarda Wireshark kullanılabilir. Bunun için kullanıcı lisanslamaya veya ücrete tabi tutulmaz. Ayrıca, bütün kaynak kodu, GPL'in altında serbest bir şekilde kullanıma açıktır.

Wireshark programı grafik ara yüzü üzerinden çalışır, ancak grafik ara yüzünü kullanmayan kullanıcılar için "TShark" yazılımı geliştirilmiştir. TShark, Wireshark ile aynı işlemlere sahip olan komut satırı sürümüdür.

Wireshark, kurulu olduğu bilgisayarda;

- Ağ trafiğinin anlık olarak izlenmesini,
- İzlenen bu trafiğin kayıt edilmesini,
- Daha sonra incelenmesini sağlamaktadır.
- Bunların dışında bir hatayı çözmek amacı içinde kullanılabilir. (Bu işlem trafik izlenerek anlık filtreleme çözümleri kullanılarak sorun saptanmaya çalışılır.)

1.2 AĞ ANALİZİ VE KULLANIM ALANLARI

Wireshark' ın günümüzün önder ağ protokol analizcisi olduğunu söylemiştik. Sistem yöneticileri, ağ mühendisleri, güvenlik mühendisleri, sistem işletmecileri ve programcılarının hepsi ağ analizini kullanmaktadır. Ağ analizi ağdaki sorunları bulmada ve gidermede, sistem konfigürasyonu yayınlamada paha biçilmez bir araçtır. Geçmişte, ağ analizcileri donanım aletlerini pahalı ve kullanımı zor bir şekilde piyasaya sürmekteydi. Ancak günümüzde, teknolojiye yeni gelişmeler yazılım tabanlı ağ analizinin gelişmesine olanak tanımıştır. Bu ağ analizini daha kullanışlı ve ucuz bir hale getirmiştir. Diğer bir açıdan bakılacak olursa, ağ analizinin yetenekleri ikiyüzlü kılıç gibidir; ağ, sistem ve güvenlik uzmanları problemleri çözmede ve ağı görüntülemeye kullansa da, “davetsiz misafirler” ağ analizini kötü amaçlar için kullanmaktadır. Ağ analizinin kullanım alanları;

- Paketlerdeki ikili veri şeklindeki bilgileri, okunabilir bir formata dönüştürmede kullanılır.
- Ağdaki problemleri çözmede kullanılır.
- Ağın performansını analiz etmek için kullanılır.
- Ağa izinsiz girenleri tespit etmede kullanılır.
- Uygulamaların gerçekleştirdiği operasyonları analiz etmede kullanılır.
- Ağ kartındaki hataları bulmada kullanılır.
- Virüslerin bulaştığını veya Denial of Service(DOS) ataklarını bulmada kullanılır.
- Risk altındaki bilgisayarları bulmada kullanılır.
- Casus yazılımları bulmada kullanılır.

- Aynı zamanda protokoller hakkında eğitici bir kaynaktır.

2. WIRESHARK KURULUMU

Bu aracı bilgisayarınızda sağlıklı bir şekilde çalıştırabilmeniz için aşağıda belirtilen sistem gereksinimlerini karşılıyor olmanız gerekmektedir;

- Universal C Runtime
- Windows 10 ve Windows Server 2019 (Eğer yoksa KB2999226 veya KB3118401'i yüklemeniz gerekir.)
- Herhangi bir modern 64-bit AMD64/x86-64 veya 32-bit x86 işlemci
- 500 MB kullanılabilir RAM. Daha büyük dosyaları için daha fazla RAM gerektirir.
- 500 MB kullanılabilir disk alanı. Büyük dosyalar için ek disk alanı gerektirir.
- Herhangi bir modern ekran. 1280×1024 veya daha yüksek çözünürlük önerilir. Wireshark, varsa HiDPI veya Retina çözünürlüklerini kullanır.
- Uzman kullanıcılar, birden fazla monitörü faydalı bulacaktır.
- İnterneti yakalamak için desteklenen bir ağ kartı
- İnternet
- Windows tarafından desteklenen herhangi bir kart çalışmalıdır. Linux, Mac için desteklenen kartlar sisteme göre olmalıdır.

2.1 WINDOWS İŞLETİM SİSTEMİNE YÜKLEME

1. <https://www.wireshark.org/#download> adresinden program indirilir.

Wireshark'ı indirin

Wireshark'ın mevcut kararlı sürümü 3.6.1'dir.

Kararlı Sürüm (3.6.1) • 29 Aralık 2021

- Windows Yükleyici (64-bit)
- Windows Yükleyici (32 bit)
- Windows PortableApps® (64-bit)
- Windows PortableApps® (32-bit)
- macOS Arm 64-bit .dmg
- macOS Intel 64-bit .dmg
- Kaynak kodu

Eski Kararlı Sürüm (3.4.11) • 29 Aralık 2021

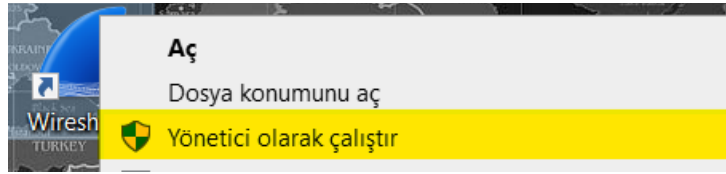
belgeler

Daha indirir ve belgeler bulunabilir [indirme sayfasına](#).

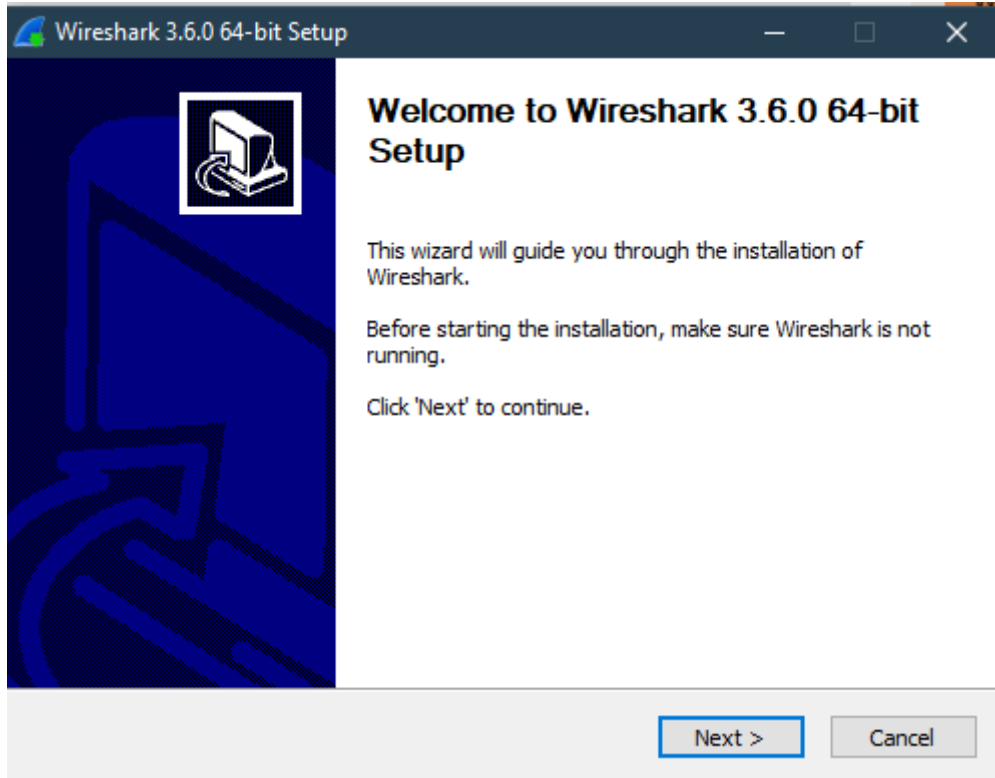
SharkFest Sponsorları

- Always-on, scalable Packet Capture that integrates with all your tools
- endace
- FMADIO
- Never Drop Packets!
- 100Gbps 148Mpps sustained 24/7
- Line Rate Full Packet Capture Hardware System
- riverbed
- MAXIMIZE YOUR DIGITAL PERFORMANCE
- RETHINK POSSIBLE
- SCOS
- WIRESHARK UNIVERSITY
- Authorized Training Partner
- Official TCP / IP Troubleshooting Course
- Training & Wireshark Tools

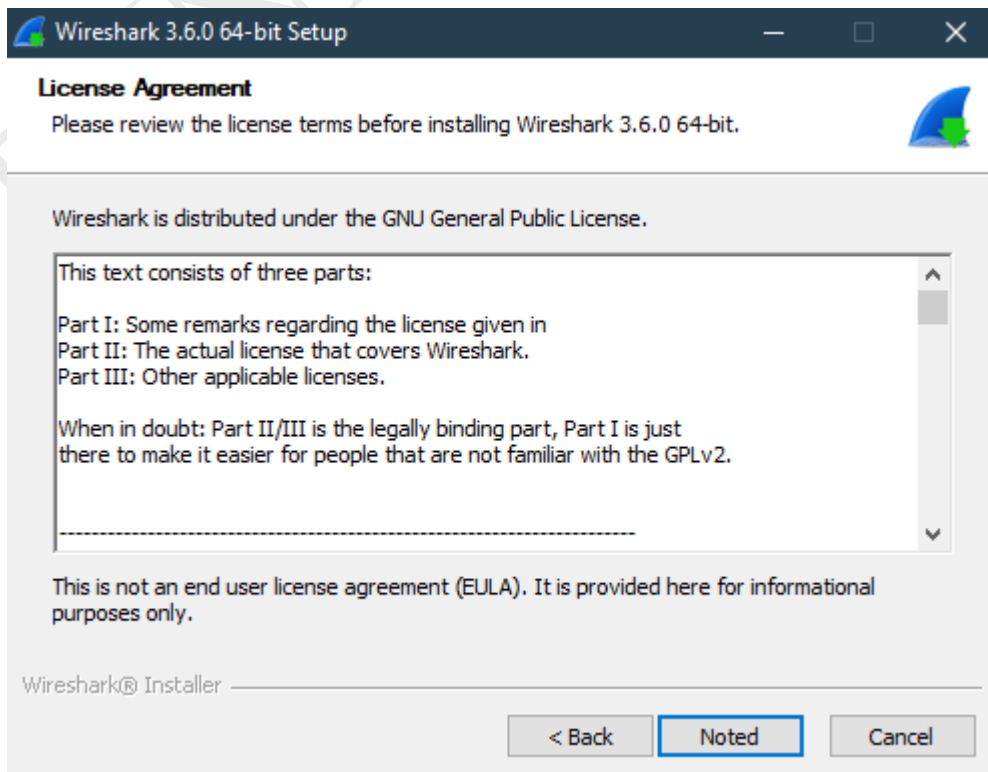
2. Kurulan dosya yönetici olarak başlatılır.



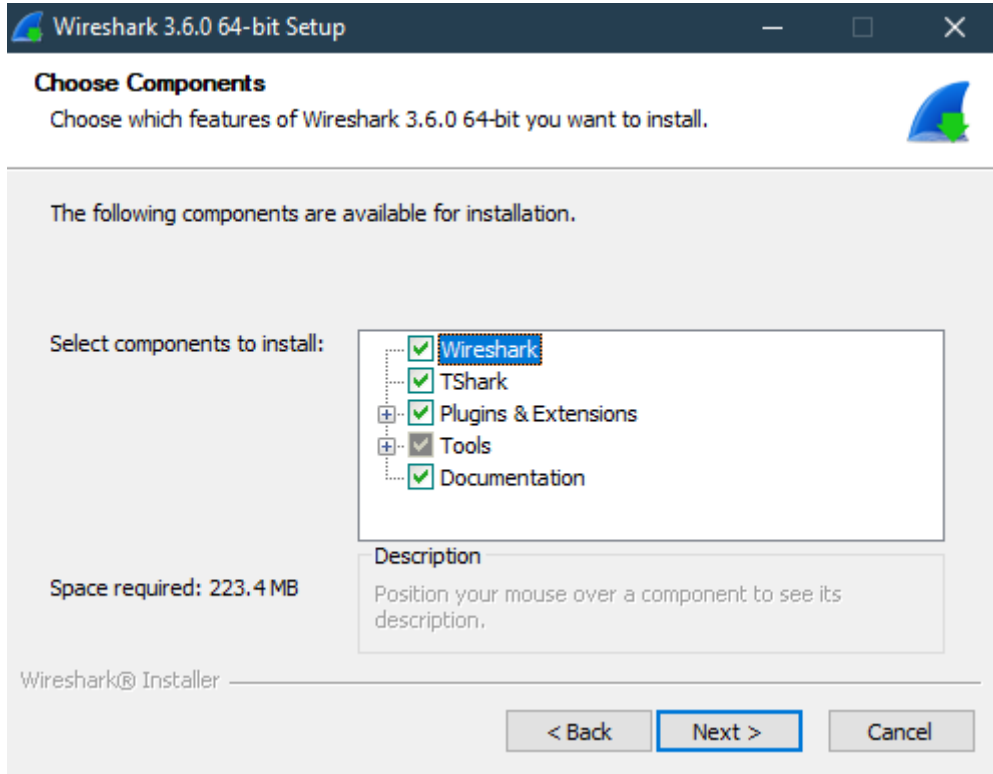
3. Kurulum sihirbazında <<Next>> denilerek devam edilir.



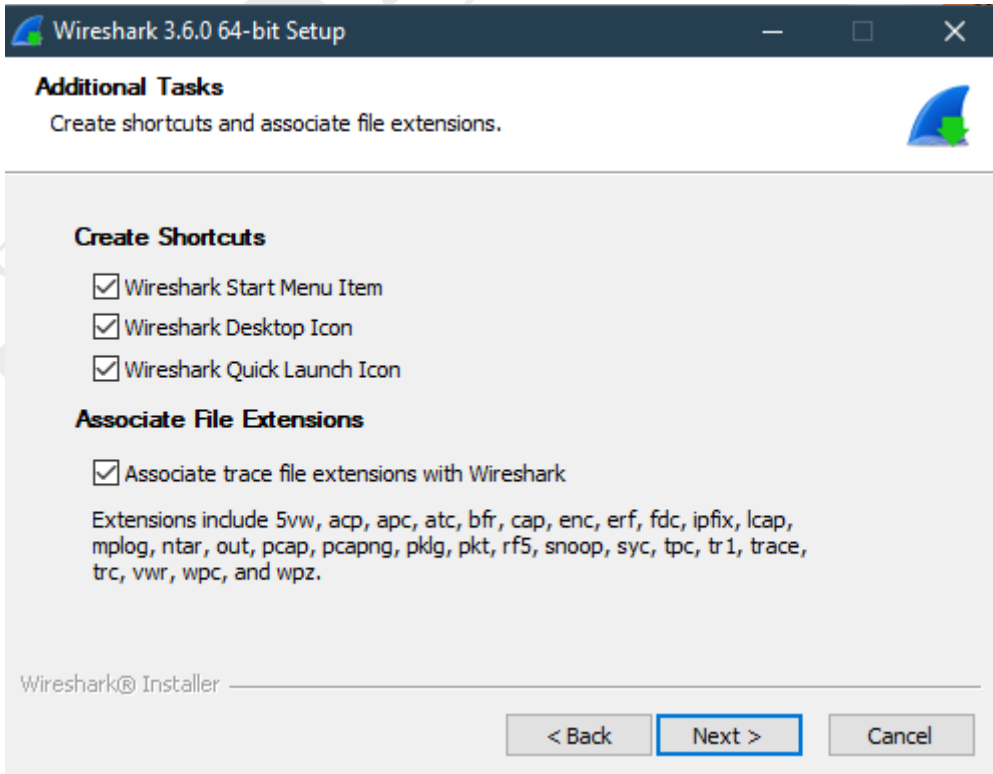
4. Lisans anlaşmasını kabul etmek için <<Noted>> tıklanarak ilerlenir.



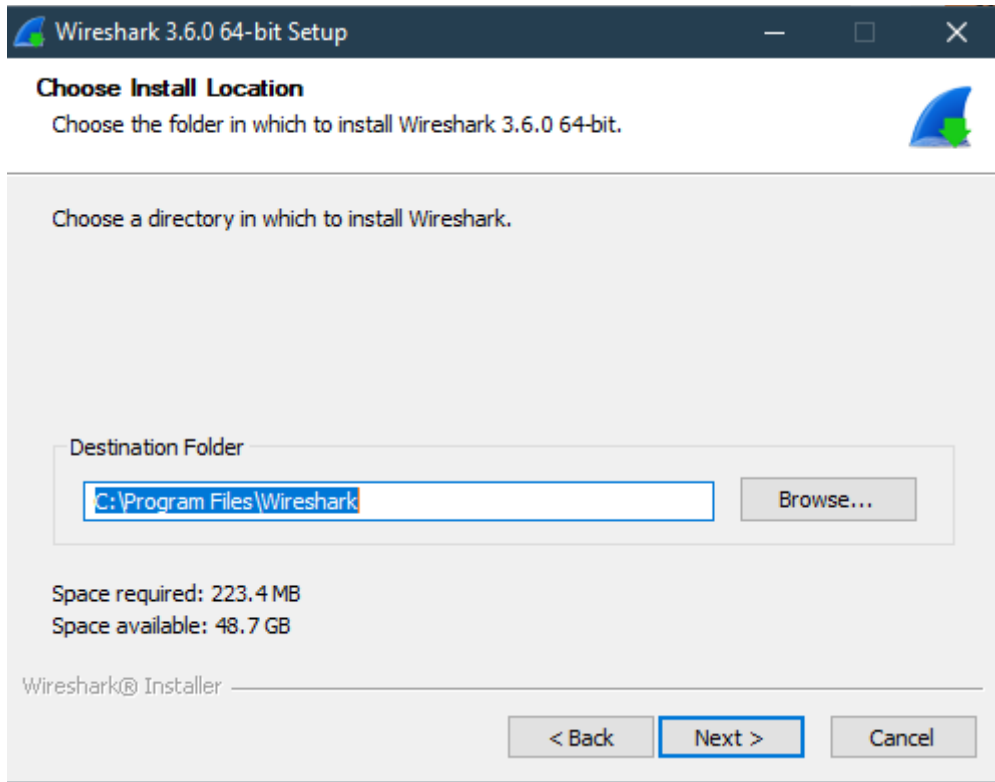
5. Bileşenler varsayılan olarak bırakılır ve devam etmek için <<Next>> butonuna tıklanarak ilerlemeye devam edilir.



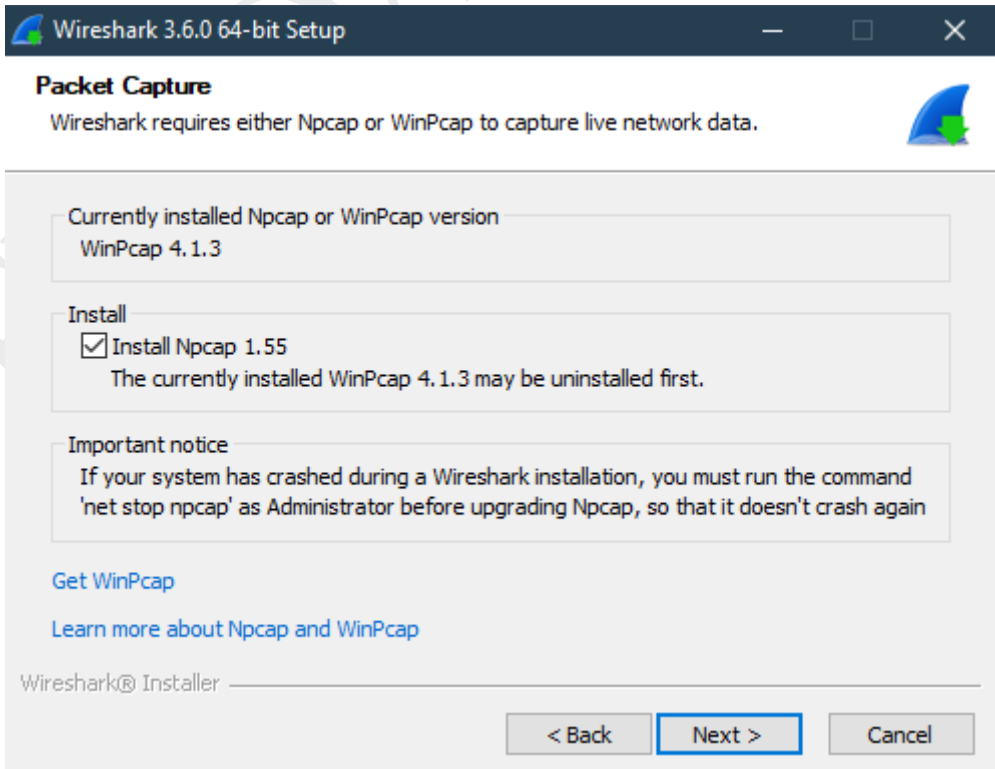
6. İstenilen ek görevler seçilir veya devre dışı bırakılarak yine <<Next>> diyerek ilerlenir.



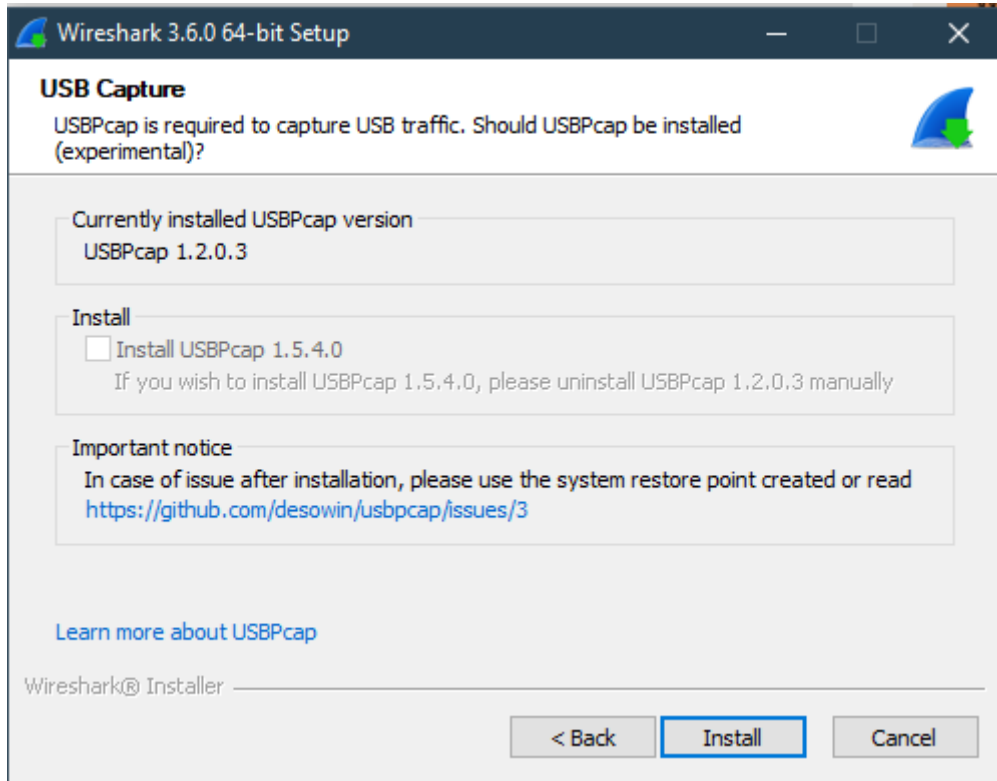
7. Kurulum lokasyonu seçilir.<<Next>> butonuna tıklanarak ilerlenir.



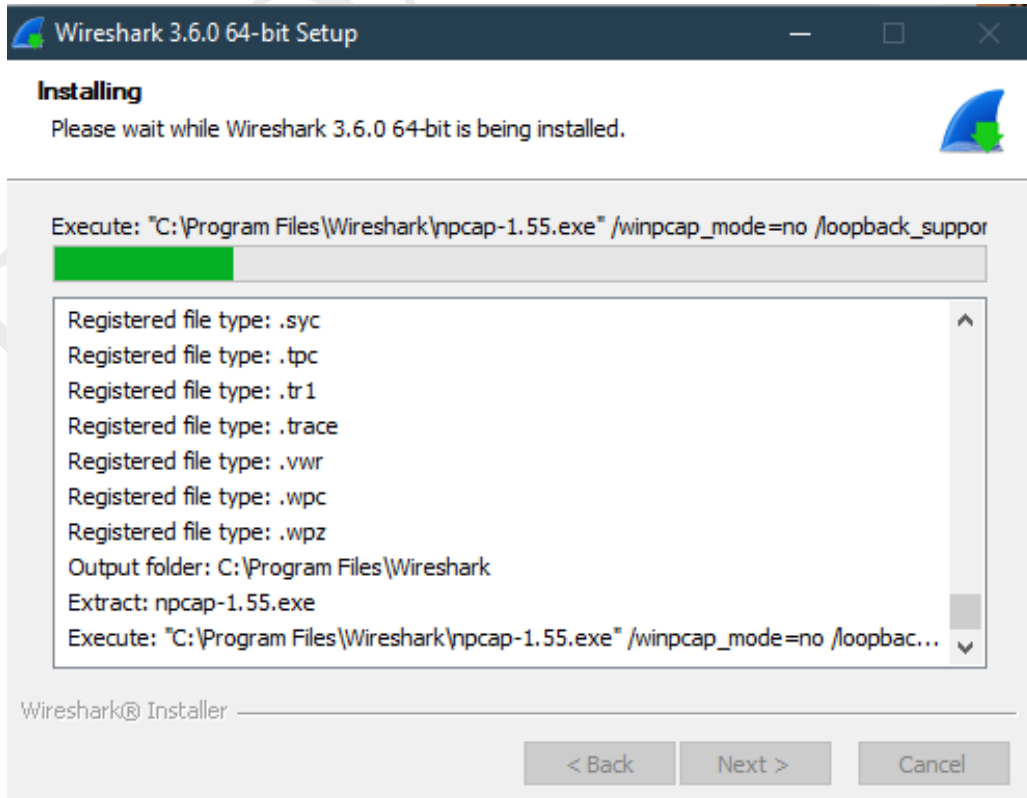
8. Npcap kurulumu yapılması için “Install Npcap 1.55” kutucuğu aktif bırakılır ve <<Next>> diyerek ilerlenir.



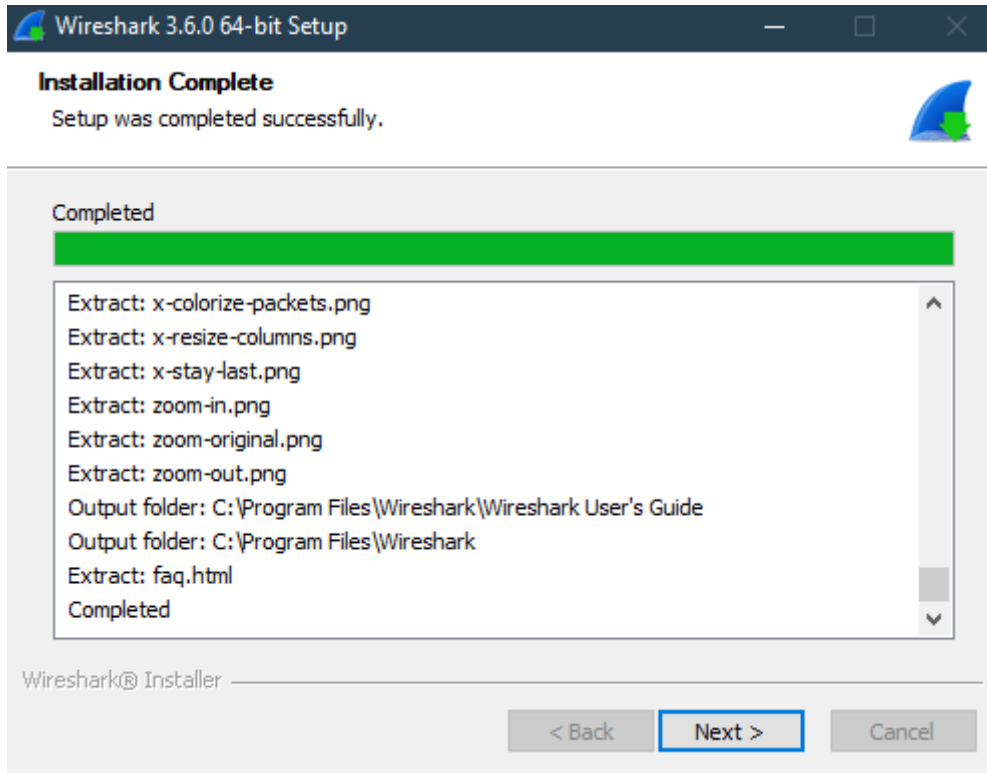
9. USBcap programı, USB aygıtlarını capture etmek için gereklidir. <<Install>> butonuna tıklanarak ilerlenir.



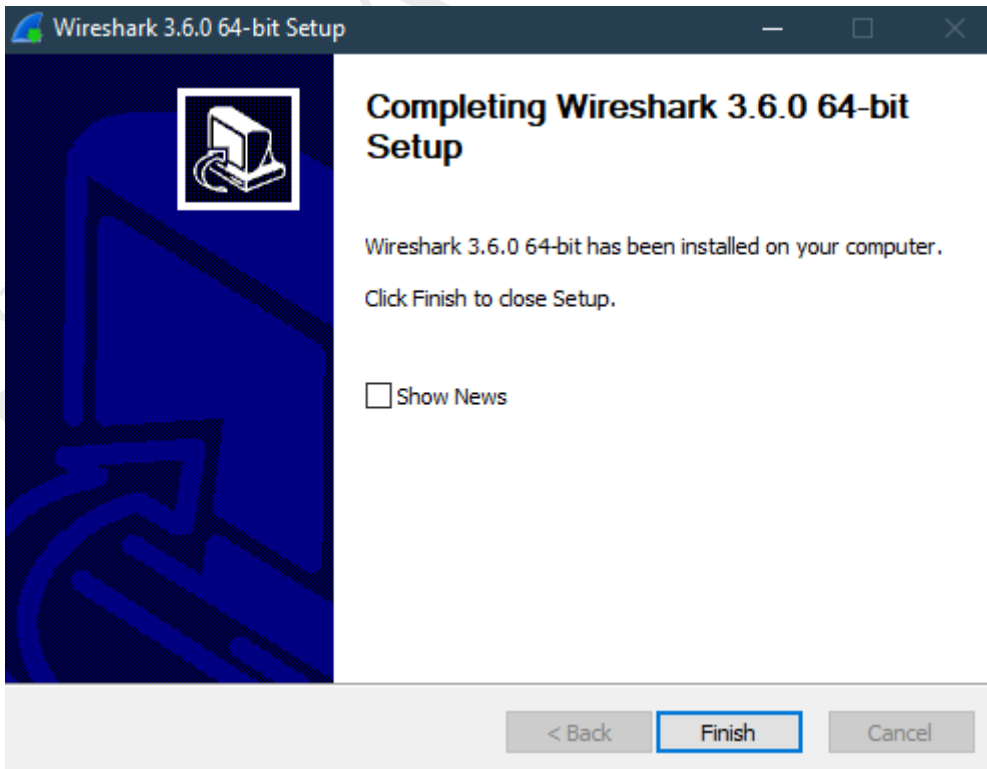
10. Gerekli doyalar ayıklanıyor ve kurulum başlatılıyor. Biraz beklenir.



11. İşlem tamamlandıktan sonra <<Next>> diyerek ilerlemeye devam edilir.



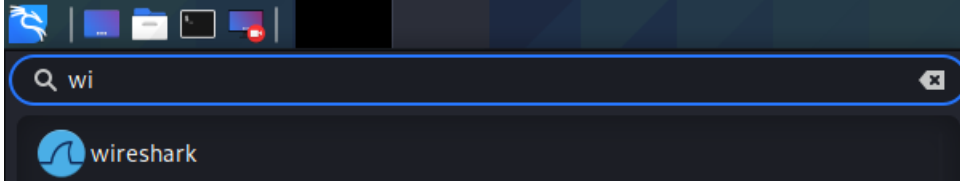
12. <<Finish>> tıklanarak kurulum işlemi tamamlanır.



2.2 LİNX İŞLETİM SİSTEMİNE YÜKLEME

Aşağıdaki kodlar sırasıyla Terminalde çalıştırılır.

- 1) `sudo add-apt-repository ppa:wireshark-dev/stable`
- 2) `sudo apt-get update`
- 3) `sudo apt-get install Wireshark`
- 4) Programın kurulumu tamamlanacaktır.



3. KULLANICI ARAYÜZ SEKMELERİ

3.1 “ANA” ARAÇ ÇUBUĞU

Ana araç çubuğu, menüden sık kullanılan öğelere hızlı erişim sağlar. Bu araç çubuğu kullanıcı tarafından özelleştirilemez, ancak daha fazla paket verisi göstermek için ekrandaki alana ihtiyaç duyulursa Görünüm menüsü kullanılarak gizlenebilir.

Araç çubuğundaki öğeler, ilgili menü öğelerine benzer şekilde etkinleştirilir veya devre dışı bırakılır (grileşir). Örneğin, aşağıdaki resimde bir dosya açıldıktan sonra ana pencere araç çubuğu gösterilmektedir. Dosyayla ilgili çeşitli düğmeler etkinleştirilir, ancak yakalama işlemi devam etmediğinden yakalamayı durdur düğmesi devre dışı bırakılır.



Son yakalamayla aynı seçeneklerle veya hiçbiri ayarlanmadıysa varsayılan seçeneklerle paketleri yakalamaya başlar



Hâlihazırda çalışan yakalamayı durdurur.



Geçerli yakalama oturumunu yeniden başlatır.



Yakalama Seçenekleri” iletişim kutusunu açar.



Görüntülemek üzere bir yakalama dosyası yüklemenizi sağlayan dosya açma iletişim kutusunu açar.



Geçerli yakalama dosyasını istediğiniz dosyaya kaydedin. Hâlihazırda geçici bir yakalama dosyanız varsa, bunun yerine “Kaydet” simgesi gösterilecektir.



Geçerli yakalamayı kapatır. Yakalamayı kaydetmediyseniz, önce kaydetmeniz istenecektir.



Geçerli yakalama dosyasını yeniden yükler.



Farklı kriterlere göre bir paket bulun.



Paket geçmişinde geri gidin.



Paket geçmişinde ileri atlayın.



Belirli bir pakete gidin.



Yakalama dosyasının ilk paketine atlayın.



Yakalama dosyasının son paketine atlayın.



Canlı yakalama yaparken otomatik kaydırma paket listesi.



Paket listesini renklendirin.



Paket verilerini yakınlaştırm (yazı tipi boyutunu artırın).



Paket verilerini uzaklaştırm (yazı tipi boyutunu küçültün).



Yakınlaştırma seviyesini tekrar %100'e ayarlayın.



Sütunları yeniden boyutlandırın, böylece içerik onlara sığar.

3.2 “FİLTRE” ARAÇ ÇUBUĞU

Bir görüntüleme filtresi uygula ... <Ctrl-/>



Kaydedilmiş filtreleri yönetin veya seçin.



Mevcut görüntü filtresini sıfırlayın ve düzenleme alanını temizleyin.



Düzenleme alanındaki mevcut değeri yeni görüntü filtresi olarak uygulayın. Büyük yakalama dosyalarına bir görüntü filtresi uygulamak oldukça uzun zaman alabilir.



Son uygulanan filtreler listesinden seçim yapın.



Yeni bir filtre düğmesi ekleyin.

Görüntü Filtresi İfadeleri Oluşturma

Wireshark, hangi paketlerin görüntüleneceğini tam olarak kontrol etmenizi sağlayan bir ekran filtresi dili sağlar. Bir protokolün veya alanın varlığını, bir alanın değerini kontrol etmek veya hatta iki alanı birbiriyle karşılaştırmak için kullanılabilirler. Bu karşılaştırmalar “ve” ve “veya” gibi mantıksal operatörlerle ve parantezler ile karmaşık ifadelerde birleştirilebilir. Aşağıdaki bölümler, ekran filtresi işlevine daha ayrıntılı olarak girecektir.

Filtre Alanlarını Görüntüle

En basit görüntüleme filtresi, tek bir protokolü görüntüleyen filtredir. Yalnızca belirli bir protokolü içeren paketleri görüntülemek için protokolü Wireshark'ın görüntü filtresi araç çubuğuna yazın. Örneğin, yalnızca TCP paketlerini görüntülemek için Wireshark'ın görüntü filtresi araç çubuğuna tcp yazın. Benzer şekilde, yalnızca belirli bir alanı içeren paketleri görüntülemek için, alanı Wireshark'ın görüntü filtresi araç çubuğuna yazın. Örneğin, yalnızca HTTP isteklerini görüntülemek için Wireshark'ın görüntüleme filtresi araç çubuğuna http.request yazın. Wireshark'ın desteklediği herhangi bir protokolü filtreleyebilirsiniz. Ayırıştırıcı o alan için bir kısaltma eklediye, bir ayırıştırıcının ağaç görünümüne eklediği herhangi bir alanı da filtreleyebilirsiniz. Kullanılabilir protokollerin ve alanların tam listesine Görünüm / Dahililer / Desteklenen Protokoller menü öğesi aracılığıyla erişilebilir.

Değerleri Karşılaştırma

Bir dizi farklı karşılaştırma operatörü kullanarak değerleri karşılaştıran görüntü filtreleri oluşturabilirsiniz.

Takma ad	Gösterim	Açıklama
any_eq	==	Eşit (birden fazla ise herhangi biri)
all_ne	!=	Eşit değil (birden fazla ise tümü)
all_eq	===	Eşit (birden fazla ise tümü)
Herhangi bir_ne	!==	Eşit değil (birden fazla ise herhangi biri)
	>	daha büyük
	<	Daha az

Takma ad	Gösterim	Açıklama
	>=	Büyük veya eşit
	<=	Küçük veya eşit
		Protokol, alan veya dilim bir değer içeriyor
	~	Protokol veya metin alanı, Perl uyumlu bir normal ifadeyle eşleşir
	&	Bit düzeyinde VE sıfırdan farklı

Filtre Alan Türlerini Görüntüle

İşaretsiz tam sayı

8, 16, 24, 32 veya 64 bit olabilir. Tam sayıları ondalık, sekizlik veya onaltılık olarak ifade edebilirsiniz. Aşağıdaki görüntü filtreleri eşdeğerdir:

- ip.len le 1500
- ip.len le 02734
- ip.len le 0x5dc

İşaretili tam sayı

8, 16, 24, 32 veya 64 bit olabilir. İşaretsiz tamsayılarda olduğu gibi ondalık, sekizlik veya onaltılık kullanabilirsiniz.

Boole

1 (doğru için) veya 0 (yanlış için) olabilir.

Değeri doğru veya yanlış olsun, bir Boole alanı mevcuttur. Örneğin tcp.flags.syn, SYN bayrağı 0 veya 1 olsun, bayrağı içeren tüm TCP paketlerinde bulunur. TCP paketlerini yalnızca SYN bayrağı seti ile eşleştirmek için kullanmanız gerekir tcp.flags.syn == 1.

Ethernet adresi

Ayırıcılar arasında bir veya iki bayt olacak şekilde iki nokta üst üste (:), nokta (.) veya kısa çizgi (-) ile ayrılmış 6 bayt:

- eth.dst == ff:ff:ff:ff:ff:ff

- eth.dst == ff-ff-ff-ff-ff-ff
- eth.dst == ffff.ffff.ffff

IPv4 adresi

- ip.addr == 192.168.0.1

Sınıfsız Etki Alanları Arası Yönlendirme (CIDR) gösterimi, bir IPv4 adresinin belirli bir alt ağda olup olmadığını test etmek için kullanılabilir. Örneğin, bu görüntü filtresi 129.111 Sınıf B ağındaki tüm paketleri bulacaktır:

- ip.addr == 129.111.0.0/16

IPv6 adresi

- ipv6.addr == ::1

IPv4 adreslerinde olduğu gibi, IPv6 adresleri bir alt ağ ile eşleşebilir.

Metin dizesi

- http.request.uri == "https://www.wireshark.org/"

Dizeler bir bayt dizisidir. Gibi işlevler lower()ASCII kullanır, aksi takdirde belirli bir kodlama varsayılmaz. Dize değişmezleri çift tırnak ile belirtilir. Karakterler ayrıca on altılı \x hh veya sekizli \ddd kullanılarak bir bayt kaçış dizisi kullanılarak da belirtilebilir ; burada h ve d sırasıyla onaltılı ve sekizli sayısal basamaklardır:

dns.qry.name contains "www.\x77\x69\x72\x65\x73\x68\x61\x72\x6b.org"

Alternatif olarak bir ham dize sözdizimi kullanılabilir. Bu tür dizeler, r veya ile öneklenir R ve ters eğik çizgiyi değişmez bir karakter olarak ele alır.

http.user_agent matches r"(X11;"

Tarih ve saat

frame.time == "Sep 26, 2004 23:18:04.954975"

ntp.xmt ge "2020-07-04 12:34:56"

Mutlak zaman alanının değeri, yukarıdaki iki biçimden biri kullanılarak bir dize olarak ifade edilir. Kesirli saniyeler atlanabilir veya nano saniye hassasiyetine kadar belirtilebilir; fazladan sondaki sıfırlara izin verilir, ancak diğer rakamlara izin verilmez. Dize bir saat dilimi son eki alamaz ve UTC'de görüntülenen alanlar için bile her zaman yerel saat diliminde olduğu gibi ayrıştırılır.

İlk formatta, kısaltılmış ay adları yerel ayardan bağımsız olarak İngilizce olmalıdır. İkinci formatta, en az anlamlıdan (saniye) en fazlaya doğru herhangi bir sayıda zaman alanı atlanabilir, ancak en azından tarihin tamamı belirtilmelidir:

frame.time < "2022-01-01"

İkinci formatta, TISO 8601'de olduğu gibi tarih ve saat arasında a görünebilir, ancak daha az önemli zamanlar atlandığında değil.

Dilim Operatörü

Wireshark, bir dizinin bir alt dizisini oldukça ayrıntılı yollarla seçmenize olanak tanır. Bir etiketten sonra, aralık belirteçlerinin virgülle ayrılmış bir listesini içeren bir çift parantez "[]" yerleştirebilirsiniz.

eth.src[0:3] == 00:00:83

Yukarıdaki örnek, tek bir aralık belirtmek için n:m biçimini kullanır. Bu durumda n başlangıç ofsetidir ve m belirtilen aralığın uzunluğudur.

eth.src[1-2] == 00:83

Yukarıdaki örnek, tek bir aralık belirtmek için nm biçimini kullanır. Bu durumda n başlangıç ofseti ve m bitiş ofsetidir.

eth.src[:4] == 00:00:83:00

Yukarıdaki örnek, bir dizinin başlangıcından m uzaklığına kadar her şeyi alan :m biçimini kullanır. 0:m'ye eşittir

eth.src[4:] == 20:20

Yukarıdaki örnek, ofset n'den dizinin sonuna kadar her şeyi alan n: biçimini kullanır.

eth.src[2] == 83

Yukarıdaki örnek, tek bir aralık belirtmek için n biçimini kullanır. Bu durumda dizideki eleman ofset n'de seçilir. Bu, n:1'e eşittir.

eth.src[0:3,1-2,:4,4:,2] ==

00:00:83:00:83:00:00:83:00:20:20:83

Wireshark, yukarıda gösterildiği gibi bileşik aralıklar oluşturmak için virgülle ayrılmış bir listede tek aralıkları bir araya getirmenize olanak tanır.

Üyelik Operatörü

Wireshark, bir alanı bir dizi değer veya alana üyelik açısından test etmenize olanak tanır. Alan adından sonra inoperatörü ve ardından { } ayrıçlarıyla çevrelenmiş küme öğelerini kullanın. Örneğin, TCP kaynağı veya 80, 443 veya 8080 hedef bağlantı noktasına sahip paketleri görüntülemek için tcp.port in {80, 443, 8080}. Küme öğeleri virgülle ayrılmalıdır. Değer kümesi ayrıca aralıklar içerebilir: tcp.port in {443,4430..4434}.

DHCP için kullanılabilecek bazı örnek filtreler;

- port 67 or port 68
- bootp
- bootp.option.dhcp == 1 (DISCOVER Packets)
- bootp.option.dhcp == 2 (OFFER Packets)
- bootp.option.dhcp == 3 (REQUEST Packets)
- bootp.option.dhcp == 4 (ACK Packets)
- bootp.option.hostname

HTTP için kullanılabilecek bazı örnek filtreler

- http.request.method=="GET"
- http.request.method=="POST"
- http.response.code == "200"
- http.user_agent == "User_Agent_Değeri"
- http.referer

ARP için kullanılabilecek bazı örnek filtreler

- arp
- arp.src.hw_mac == "Kaynak mac adresi"
- arp.dst.hw_mac == "Hedef mac adresi"
- arp.duplicate-address-frame
- arp.opcode == 1
- arp.opcode == 2

DNS için kullanılabilecek bazı örnek filtreler

- dns.qry.name == "google.com"
- "dns.qry.type == 1 (A Record Type)dns.qry.type == 255 (ANY Record Type)"
- dns.qry.type == 2 (NS name server)dns.qry.type == 15(MX mail exchange)
- dns

İnternet Protokol için kullanılabilecek bazı örnek filtreler

- ip.addr
- ip.ttl
- ip.version == 4
- ip.src == 192.168.2.45
- ip.dst == 192.168.2.34

ICMP için kullanılabilecek bazı örnek filtreler

- icmp.type
- icmp.code

3.3 “PAKET LİSTESİ” BÖLMESİ

Geçerli yakalama dosyasındaki tüm paketleri görüntüler.

No.	Time	Source	Destination	Protocol	Length	Info
1257	1149.056188	51.91.80.48	192.168.1.8	TCP	54	[TCP Keep-Alive] 80 → 64405 [ACK] Seq=1 Ack=1 Win=501 Len=0
1258	1149.056256	192.168.1.8	51.91.80.48	TCP	54	[TCP Keep-Alive ACK] 64405 → 80 [ACK] Seq=1 Ack=2 Win=510 Len=0
1259	1152.304563	192.168.1.8	51.91.80.48	TCP	55	[TCP Keep-Alive] 64405 → 80 [ACK] Seq=0 Ack=2 Win=510 Len=1
1260	1152.432016	51.91.80.48	192.168.1.8	TCP	66	[TCP Keep-Alive ACK] 80 → 64405 [ACK] Seq=2 Ack=1 Win=501 Len=0 SLE=0 SRE=1
1261	1161.296871	192.168.1.8	108.177.119.188	TCP	55	[TCP Keep-Alive] 64430 → 5228 [ACK] Seq=27 Ack=27 Win=509 Len=1
1262	1161.448006	108.177.119.188	192.168.1.8	TCP	66	[TCP Keep-Alive ACK] 5228 → 64430 [ACK] Seq=27 Ack=28 Win=265 Len=0 SLE=27 SRE=28
1263	1162.673477	51.91.80.48	192.168.1.8	TCP	54	[TCP Keep-Alive] 80 → 64405 [ACK] Seq=1 Ack=1 Win=501 Len=0
1264	1162.673541	192.168.1.8	51.91.80.48	TCP	54	[TCP Keep-Alive ACK] 64405 → 80 [ACK] Seq=1 Ack=2 Win=510 Len=0
1265	1168.616654	192.168.1.9	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1266	1169.538664	192.168.1.9	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1267	1170.556493	192.168.1.9	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1268	1171.589491	192.168.1.9	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1269	1172.006814	192.168.1.2	224.0.0.251	MDNS	161	Standard query 0x0000 ANY {"nm":"Redmi Note 8","as":["8193, 8194"],"ip":"2"}._mi-connect._udp.local, "QU" question SRV 0 0 56666 ...
1270	1172.006814	fe80::8213:3289:1f2...	ff02::fb	MDNS	181	Standard query 0x0000 ANY {"nm":"Redmi Note 8","as":["8193, 8194"],"ip":"2"}._mi-connect._udp.local, "QU" question SRV 0 0 56666 ...

Paket listesindeki her satır, yakalama dosyasındaki bir pakete karşılık gelir. Bu bölmede bir satır seçerseniz, “Paket Ayrıntıları” ve “Paket Baytları” bölmelerinde daha fazla ayrıntı görüntülenecektir. Bir paketi incelerken Wireshark, protokol ayrıştırıcılarından gelen bilgileri sütunlara yerleştirir. Daha yüksek seviyeli protokoller daha düşük seviyelerdeki bilgilerin üzerine yazabileceğinden, genellikle sadece mümkün olan en yüksek seviyeden gelen bilgileri görürsünüz.

Çok sayıda farklı sütun mevcuttur. Hangi sütunların görüntüleneceği tercih ayarlarıyla seçilebilir. Varsayılan sütunlar şunları gösterecektir:

- No(Hayır)

Yakalama dosyasındaki paketin numarası. Bu sayı, bir ekran filtresi kullanılsa bile değişmez.

- Time(Zaman)

Paketin zaman damgası, bu zaman damgasının sunum formatı değiştirilebilir,

- Source(Kaynak)

Bu paketin geldiği adres

- Destination(Hedef)

Bu paketin gideceği adres

- Protocol(Protokol)

Kısa bir versiyonda ki protokol adı

- Length(Uzunluk)

Her paketin uzunluğu

- Info

Bilgi Paket içeriği hakkında ek bilgi.

İlgili Paket Sembolleri



Bir konuşmadaki ilk paket



Seçilen konuşmanın bir parçası



Seçilen konuşmanın bir parçası değil



Bir konuşmadaki son paket



Rica etmek



Tepki



Seçilen paket bu paketi onaylar.



Seçilen paket, bu paketin yinelenen bir onayıdır.



Seçilen paket, bu paketle başka bir şekilde, örneğin yeniden birleştirmenin bir parçası olarak ilişkilidir.

3.4 “PAKET AYRINTILARI” BÖLMESİ

Paket ayrıntıları bölümü, mevcut paketi (“Paket Listesi” bölümünde seçilen) daha ayrıntılı bir biçimde gösterir.

```
> Frame 1: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface \Device\NPF_{F0E20BAC-B3A5-4E07-8404-4DE10845623B}, id 0
> Ethernet II, Src: CloudNet_31:b8:5b (48:5f:99:31:b8:5b), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 62900, Dst Port: 1900
v Simple Service Discovery Protocol
  > M-SEARCH * HTTP/1.1\r\n
    HOST: 239.255.255.250:1900\r\n
    MAN: "ssdp:discover"\r\n
    MX: 1\r\n
    ST: urn:dial-multiscreen-org:service:dial:1\r\n
    USER-AGENT: Google Chrome/96.0.4664.110 Windows\r\n
    \r\n
    [Full request URI: http://239.255.255.250:1900*]
    [HTTP request 1/1]
```

Bazı protokol alanlarının özel anlamları vardır.

Oluşturulan alanlar: Wireshark'ın kendisi, yakalanan verilerde bulunmayan ek protokol bilgileri üretecektir. Bu bilgi köşeli parantez (“[” ve “]”) içine alınmıştır. Üretilen bilgiler, yanıt sürelerini, TCP analizini, IP konum belirleme bilgilerini ve sağlama toplamı doğrulamasını içerir.

Bağlantılar: Wireshark, yakalama dosyasında başka bir paketle bir ilişki algılasa, o pakete bir bağlantı oluşturur. Bağlantıların altı çizilir ve mavi renkte görüntülenir. Bir bağlantıya çift tıkladıysanız, Wireshark ilgili pakete atlayacaktır.

3.5 “PAKET BAYTLARI” BÖLMESİ

Paket bayt bölmesi, geçerli paketin (“Paket Listesi” bölümünde seçilen) verilerini hexdump stilinde gösterir.

0000	48 5f 99 31 b8 5b e8 5a 8b 36 ca ff 08 00 45 00	H_1.[.Z .6....E.
0010	00 93 5f 0b 40 00 ff 11 79 a8 c0 a8 01 02 e0 00	.._@... y.....
0020	00 fb 14 e9 14 e9 00 7f 74 4f 00 00 00 00 00 01 t0.....
0030	00 00 00 01 00 00 32 7b 22 6e 6d 22 3a 22 52 652{ "nm": "Re
0040	64 6d 69 20 4e 6f 74 65 20 38 22 2c 22 61 73 22	dmi Note 8", "as"
0050	3a 22 5b 38 31 39 33 2c 20 38 31 39 34 5d 22 2c	:"[8193, 8194]",
0060	22 69 70 22 3a 22 32 22 7d 0b 5f 6d 69 2d 63 6f	"ip": "2" }._mi-co
0070	6e 6e 65 63 74 04 5f 75 64 70 05 6c 6f 63 61 6c	nnect._u dp.local
0080	00 00 ff 00 01 c0 0c 00 21 00 01 00 00 00 78 00 !.....x.
0090	10 00 00 00 00 dd 5a 07 41 6e 64 72 6f 69 64 c0Z. Android.

Her satır, veri ofsetini, on altı onaltılık baytı ve on altı ASCII baytı içerir. Yazdırılamayan baytlar bir nokta (“.”) ile değiştirilir.

Paket verilerine bağlı olarak, bazen birden fazla sayfa kullanılabilir, örneğin Wireshark bazı paketleri tek bir veri yığını halinde yeniden birleştirdiğinde. (Ayrıntılar için bkz. Bölüm 7.8, “Paketin Yeniden Birleştirilmesi”). Bu durumda, bölmenin altındaki ilgili sekmeye tıklayarak her bir veri kaynağını görebilirsiniz.

Varsayılan görüntüleme modu, fare imlecinin yukarıda gezindiği bir alanın baytlarını vurgulayacaktır. Vurgu, hareket ettikçe fare imlecini takip edecektir. Bu vurgulama gerekli değilse veya istenmiyorsa, işlevi devre dışı bırakmak için iki yöntem vardır:

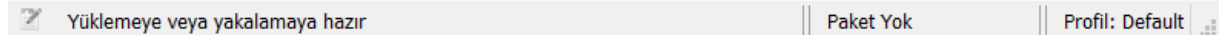
Geçici Fareyi hareket ettirirken Ctrl düğmesini basılı tuttuğunuzda, vurgulanan alan değişmez

Kalıcı olarak Bağlam menüsünü kullanarak (sağ fare tıklaması), vurgulu vurgu etkinleştirilebilir/devre dışı bırakılabilir. Bu ayar, seçilen profil son dosyasında saklanır.

3.6 DURUM ÇUBUĞU

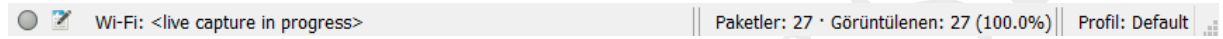
Durum çubuğu bilgi mesajlarını görüntüler. Genel olarak, sol taraf bağlamla ilgili bilgileri, orta kısım mevcut yakalama dosyası hakkındaki bilgileri ve sağ taraf seçilen yapılandırma profilini gösterir. Boyutu değiştirmek için tutamaçları metin alanları arasında sürükleyin.

- İlk Durum Çubuğu



Bu durum çubuğu, örneğin Wireshark başlatıldığında, hiçbir yakalama dosyası yüklenmediğinde gösterilir.

- Yüklü bir yakalama dosyası içeren Durum Çubuğu



O anda yüklü olan yakalama dosyasında bulunan en yüksek uzman bilgi seviyesini gösterir. Fareyi bu simgenin üzerine getirmek, uzman bilgisi seviyesinin bir açıklamasını gösterecek ve simgeye tıklamak, Uzman Bilgileri iletişim kutusunu getirecektir.

Yakalama Dosyası Özellikleri iletişim kutusunu kullanarak yakalama dosyasına bir yorum eklemenizi sağlar.

3.7 AÇILIR MENÜLER

“Paket Listesi” Sütun Başlığının Açılır Menüsü

The screenshot shows the Wireshark interface with the 'Paket Listesi' (Packet List) pane. The context menu is open over the 'Info' column header. The menu options are:

- Sola Hizala
- Ortaya Hizala
- Sağa Hizala
- Sütun Tercihleri...
- Sütunu Düzenle
- İçeriği Yeniden Boyutlandır
- Sütunu Genişliğe Yeniden Boyutlandır...
- Adları Çöz
- No.
- Time
- Source
- Destination
- Protocol
- Length
- Info
- Bu Sütunu Kaldır

The 'Info' option is currently selected. The background shows the packet list with columns: No., Time, Source, Destination, Protocol, Length, and Info. The packet list contains several entries, including a packet from 192.168.1.8 to 192.168.1.8.

Sola hizala: Bu sütundaki değerleri sola hizalayın.

Ortaya hizala: Bu sütundaki değerleri ortala hizalayın.

Sağa hizala: Bu sütundaki değerleri sağa hizalayın.

Sütun Tercihleri: Bu sütun için "Tercihler" iletişim kutusunu açın.

Sütunu Düzenle: Bu sütun için sütun düzenleyici araç çubuğunu açın.

İçeriğe Yeniden Boyutlandır: Sütunu değerlerine uyacak şekilde yeniden boyutlandırın.

Adları Çöz: Bu sütun adresleri içeriyorsa, bunları çözün.

No, Time, Source...: Ögesini seçerek bir sütunu gösterin veya gizleyin.

Sütunu kaldır: Bu sütunu, "Tercihler" iletişim kutusunda silmeye benzer şekilde kaldırın.

“Paket Listesi” Bölmesinin Açılır Menüsü

Destination	Protocol	Length	Info
239.255.255.250	SSDP	449	NOTIFY * HTTP/1.1
239.255.255.250	SS		Paket(ler)i İşaretle/İşaretini Kaldır Ctrl+M
239.255.255.250	SS		Paket(ler)i Yoksay/Yoksay Ctrl+D
239.255.255.250	SS		Zaman Referansını Ayarla/Ayarlamayı Kaldır Ctrl+T
224.0.0.251	MD		Zaman Kaydırması... Ctrl+Shift+T
ff02::fb	MD		Paket Yorumları
192.168.1.8	TC		Çözümlenen Adı Düzenle
51.91.80.48	TC		Filtre Olarak Uygula
108.177.119.188	TC		Filtre Olarak Hazırla
192.168.1.8	TC		Konuşma Filtresi
51.91.80.48	TC		Konuşmayı Renklendir
192.168.1.8	TC		SCTP
51.91.80.48	TC		Takip
66 bytes captured (528 b			Kopyala
69:d1:2b:e5:fc), Dst: Cl			Protokol Tercihleri
80.48, Dst: 192.168.1.8			Kodu Çöz...
80, Dst Port: 64405, Sec			Paketi Yeni Pencerde Göster

Paket(ler)i İşaretle/İşaretini Kaldır: Bir paketi işaretleyin veya işaretini kaldırın.

Paket(ler)i Yoksay: Yakalama dosyasını incelerken bu paketi yok sayın veya inceleyin.

Zaman Referansını Ayarla: Bir zaman referansı ayarlayın veya sıfırlayın.

Paket Yorumları: Tek bir pakete yorum eklemenizi sağlayan "Paket Yorumu" iletişim kutusunu açar. Paket yorumlarını kaydetme yeteneğinin dosya biçiminize bağlı olduğunu unutmayın. Örneğin, pcapng yorumları destekler, pcap desteklemez.

Çözümlenen Adı Düzenle: Seçili adres için çözümlemek üzere bir ad girmenizi sağlar.

Filtre Olarak Uygula: En son paket listesine veya seçilen paket ayrıntıları ögesine göre geçerli görüntü filtresini hemen değiştirin veya ekleyin. İlk alt menü ögesi filtreyi gösterir ve sonraki öğeler, filtrenin uygulanabileceği farklı yolları gösterir.

Filtre Olarak Hazırla: Geçerli görüntü filtresini, seçilen en son paket listesine veya paket ayrıntıları ögesine göre değiştirin, ancak uygulamayın. İlk alt menü ögesi filtreyi gösterir ve sonraki öğeler, filtrenin değiştirilebileceği farklı yolları gösterir.

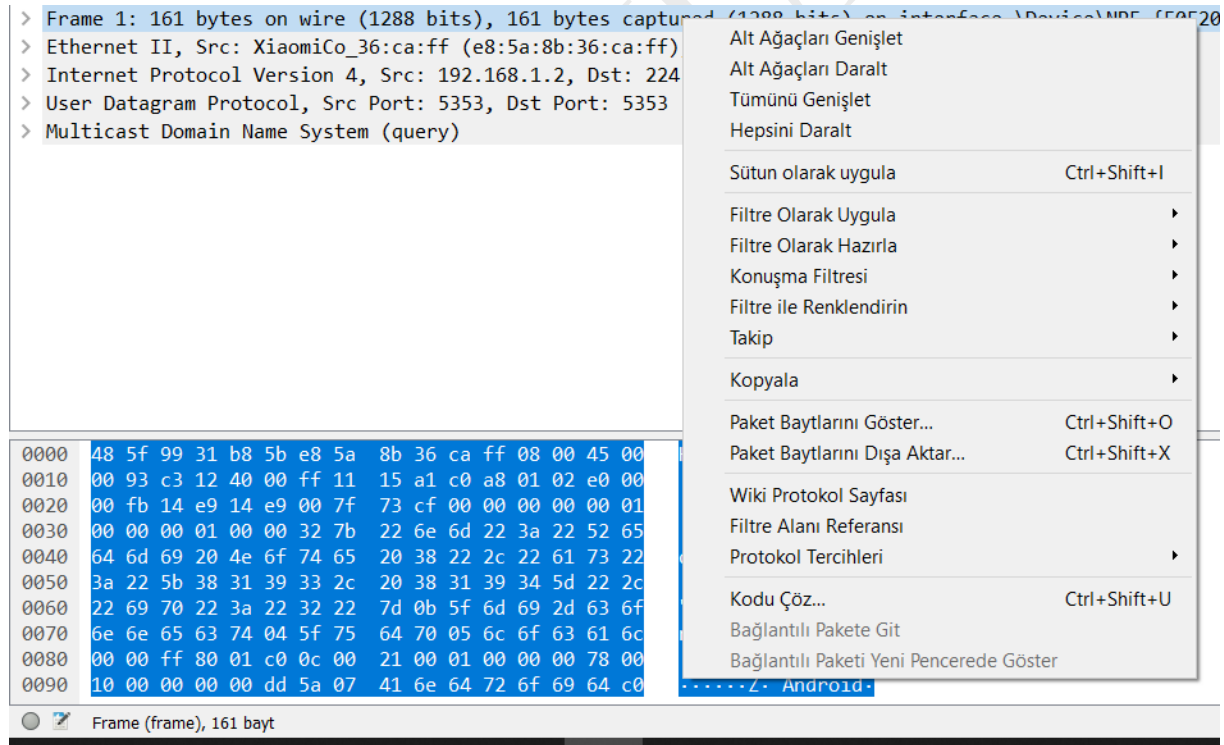
Konuşma Filtresi: Seçili paketteki adres bilgileriyle bir görüntüleme filtresi uygulayın. Örneğin, IP menüsü girişi, mevcut paketin iki IP adresi arasındaki trafiği göstermek için bir filtre ayarlayacaktır.

Konuşmayı Renklendir: Seçili paketteki adres bilgilerine dayalı olarak yeni bir renklendirme kuralı oluşturun.

SCTP: Bu SCTP ilişkilendirmesi için bir filtreyi analiz etmenize ve hazırlamanıza izin verir.

Kodu Çöz: İki disektör arasında yeni bir ilişki değiştirin veya uygulayın.

“Paket Ayrıntıları” Bölmesinin Açılır Menüsü



Alt Ağaçları Genişlet: Seçili olan alt ağacı genişletin.

Alt Ağaçları Daralt: Seçili olan alt ağacı daraltın.

Hepsini Genişlet: Yakalamadaki tüm paketlerdeki tüm alt ağaçları genişletin.

Hepsini Daralt: Wireshark, genişletilen tüm protokol alt ağaçlarının bir listesini tutar ve bir paketi görüntülediğinizde doğru alt ağaçların genişletilmesini sağlamak için bunu kullanır. Bu menü ögesi, yakalama listesindeki tüm paketlerin ağaç görünümünü daraltır.

Sütun Olarak Uygula: Paket listesinde yeni bir sütun oluşturmak için seçilen protokol ögesini kullanın.

Filtre Olarak Uygula: En son paket listesine veya seçilen paket ayrıntıları ögesine göre geçerli görüntü filtresini hemen değiştirin veya ekleyin. İlk alt menü ögesi filtreyi gösterir ve sonraki ögeler, filtrenin uygulanabileceği farklı yolları gösterir.

Filtre Olarak Hazırla: Geçerli görüntü filtresini, seçilen en son paket listesine veya paket ayrıntıları ögesine göre değiştirin, ancak uygulamayın. İlk alt menü ögesi filtreyi gösterir ve sonraki ögeler, filtrenin değiştirilebileceği farklı yolları gösterir.

Filtre ile Renklendirin: Bu menü ögesi, yeni bir renklendirme kuralı oluşturmak için seçilen protokol ögesinden gelen bilgilerle bir görüntü filtresi kullanır.

Takip edin / TCP Akışı: Seçilen paketle aynı TCP bağlantısında bulunan tüm TCP segmentlerini görüntüleyen bir pencere açın.

Takip et /UDP Akışı: "TCP Akışını İzle" ile aynı işlevsellik, ancak UDP "akışları" için.

Takip edin /TLS Akışı: "TCP Akışını İzle" ile aynı işlevsellik, ancak TLS veya SSL akışları içindir.

Takip edin / HTTP Akışı: "TCP Akışını İzle" ile aynı işlevsellik, ancak HTTP akışları içindir.

Kopyala /Tüm Görünür Öğeler:Paket ayrıntılarını görüntülediği gibi kopyalayın.

Kopyala /Tüm Görünür Seçili Ağaç Öğeler: Seçili paket ayrıntısını ve alt öğelerini görüntülediği gibi kopyalayın.

Kopyala / Açıklama: Seçili alanın görüntülenen metnini sistem panosuna kopyalayın.

Kopyala /Alan Adı: Seçili alanın adını sistem panosuna kopyalayın.

Kopyala / Değer: Seçili alanın değerini sistem panosuna kopyalayın.

Kopyala / Filtre Olarak: Seçili öğeye göre bir ekran filtresi hazırlayın ve panoya kopyalayın.

Kopyala / Onaltılık Olarak Bayt + ASCII Dökümü: Paket baytlarını tam "hexdump" formatında panoya kopyalayın.

Kopyala /...Hex Dump olarak: Paket baytlarını ASCII kısmı olmadan "hexdump" formatında panoya kopyalayın.

Kopyala / ...Yazdırılabilir Metin Olarak: Paket baytlarını, yazdırılamayan karakterler hariç, ASCII metni olarak panoya kopyalayın.

Kopyala / ...Onaltılı Akış olarak: Paket baytlarını, noktalamasız onaltılık rakamlar listesi olarak panoya kopyalayın.

Kopyala / ...Ham İkili Olarak: Paket baytlarını ham ikili olarak panoya kopyalayın. Veriler, MIME tipi “application/octet-stream” kullanılarak panoda saklanır.

Kopyala /... Kaçan Dize olarak: Paket baytlarını C tarzı kaçış dizileri olarak panoya kopyalayın.

Paket Baytlarını Dışa Aktar:

Dosya: Bu menü öğesi, aynı adı taşıyan Dosya menü öğesiyle aynıdır. Ham paket baytlarını bir ikili dosyaya aktarmanıza izin verir.

Wiki Protokol Sayfası: Web tarayıcınızda o anda seçili protokole karşılık gelen wiki sayfasını gösterin.

Filtre Alanı Referansı: Web tarayıcınızda seçili olan protokole karşılık gelen filtre alanı referans web sayfasını gösterin.

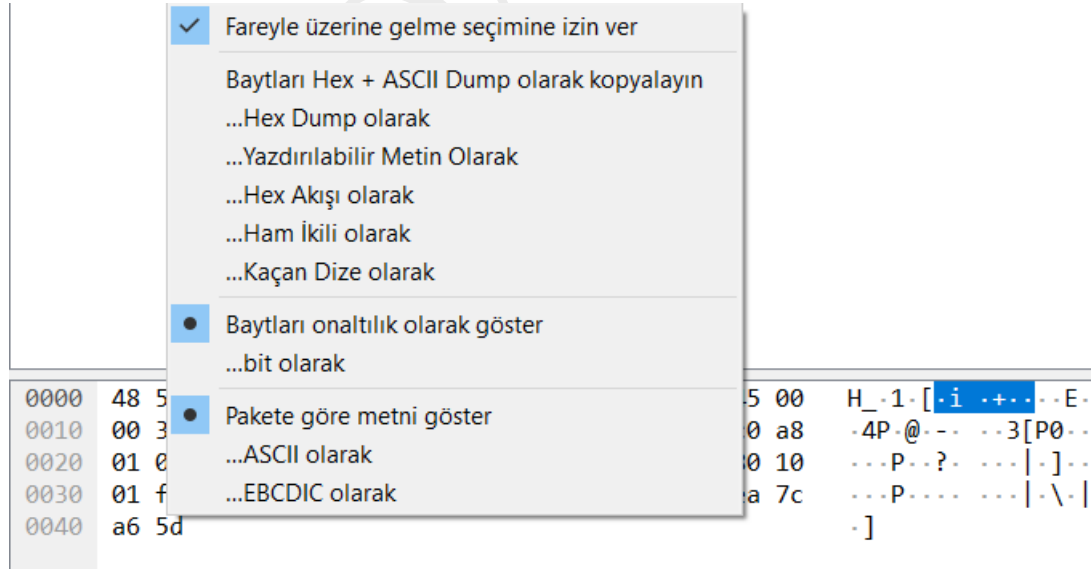
Protokol Tercihleri: Seçilen protokol için tercihleri ayarlayın.

Kodunu Çöz: İki disektör arasında yeni bir ilişki değiştirin veya uygulayın.

Bağlantılı Pakete Git: Seçilen alan, bir DNS yanıtı için eşleşen istek gibi karşılık gelen bir pakete sahipse, ona gidin.

Bağlantılı Paketi Yeni Pencerede Göster: Seçili alan, bir DNS yanıtı için eşleşen istek gibi karşılık gelen bir pakete sahipse, seçili paketi ayrı bir pencerede gösterin.

“Paket Baytları” Bölmesinin Açılır Menüsü



Baytları Hex + ASCII Dump olarak kopyalayın: Paket baytlarını tam "hexdump" formatında panoya kopyalayın.

...Hex Dump olarak: Paket baytlarını ASCII kısmı olmadan “hexdump” formatında panoya kopyalayın.

...**Yazdırılabilir Metin Olarak:** Paket baytlarını, yazdırılamayan karakterler hariç, ASCII metni olarak panoya kopyalayın.

...**Hex Akışı olarak:** Paket baytlarını, noktalamasız onaltılık rakamlar listesi olarak panoya kopyalayın.

... **Ham İkili olarak:** Paket baytlarını ham ikili olarak panoya kopyalayın. Veriler, MIME tipi “application/octet-stream” kullanılarak panoda saklanır.

... **Kaçan Dize olarak:** Paket baytlarını C tarzı kaçış dizileri olarak panoya kopyalayın.

Baytları onaltılık olarak göster: Bayt verilerini onaltılık basamaklar olarak görüntüleyin.

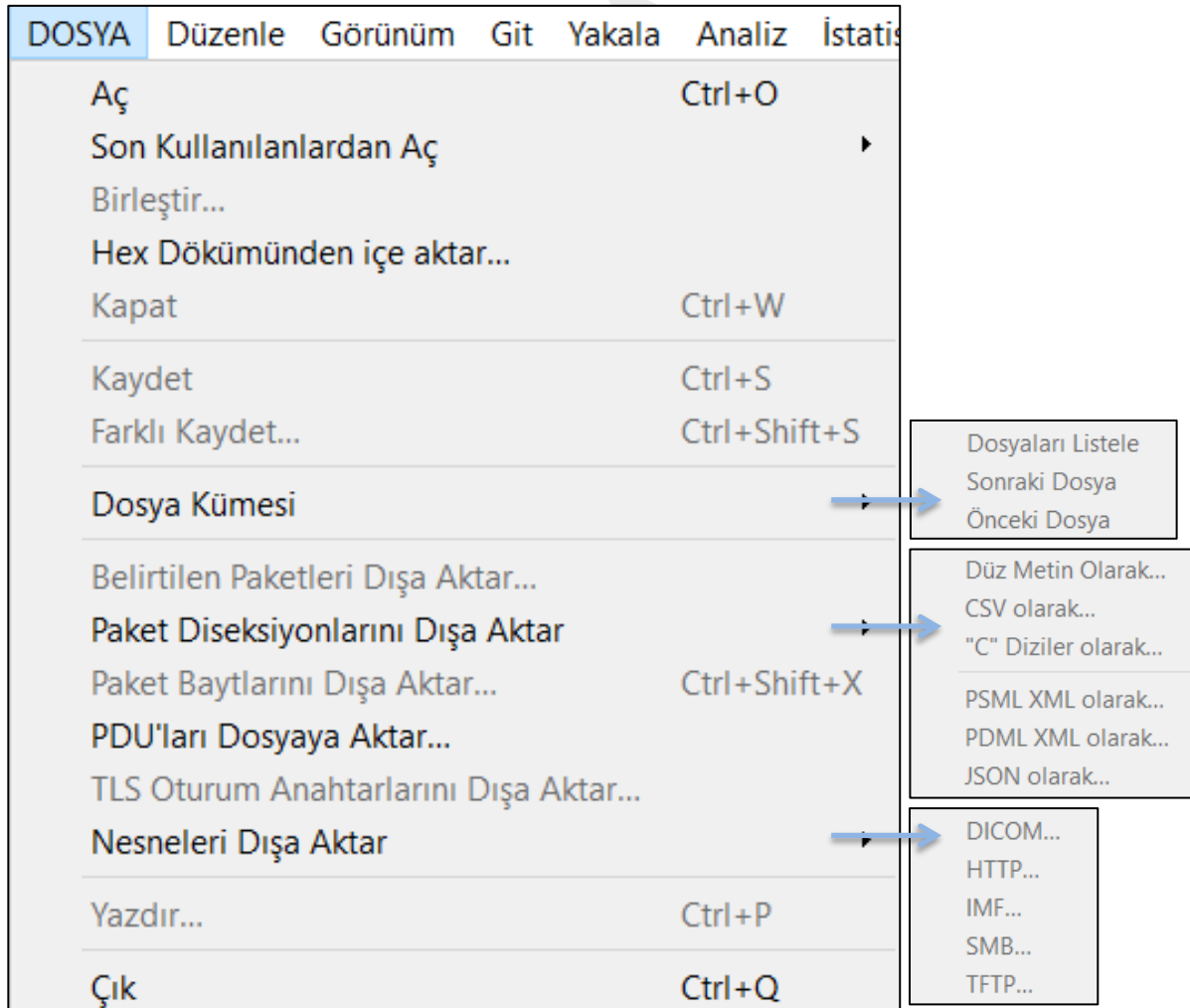
Baytları bit olarak göster: Bayt verilerini ikili rakamlar olarak görüntüleyin.

Pakete dayalı metni göster: “Hexdump” verilerini metinle gösterin.

...**ASCII olarak:** “Hexdump” metnini görüntülerken ASCII kodlamasını kullanın.

...**EBCDIC olarak:** “Hexdump” metnini görüntülerken EBCDIC kodlamasını kullanın.

3.8 DOSYA MENÜSÜ



Aç: Ctrl+O kısayol tuşlarıyla çalışır. Hazırda var olan önceden kaydedilmiş wireshark ya da başka desteklediği paket analiz yazılımlarının ürettiği dosyaları görüntülemek için kullanılır.

Son Dosyayı Aç: Son kullanılan dosyaları açmada kolaylık sağlar.

Birleştir: Kaydedilmiş dosyaları birleştirmede kullanılır.

Kapat: Ctrl+W kısayol tuşlarıyla çalışır. Açık olan dosyadan çıkar.

Kaydet: Ctrl+S kısayol tuşlarıyla çalışır. Görüntülenmekte olan paketleri kaydeder.

Farklı Kaydet: Ctrl+Shift+S kısayol tuşlarıyla çalışır. Farklı kaydeder.

Dosya Kümesi;

Dosyaları Listele: Dosya listesini oluşum tarihi, son değişim tarihi, boyutu şeklinde dosya dizisi içerisinde gösterir.

Sonraki Dosya: Dosya dizisi içinde var olanı kapatıp sonrakine atlar.

Önceki Dosya: Dosya dizisi içinde var olanı kapatıp bir öncekine atlar.

Paket Diseksiyonları Dışarı Aktar menüsü;

Düz Metin olarak: Toplanan paketleri metin dosyası olarak dışa aktarmaya yarar. Özet ve ayrıntı bölümlerini aktarır.

CSV olarak: Wireshark özet bölümündeki bilgileri virgülle ayrılmış şekilde düz metin dosyası olarak dışa aktarır.

“C” Diziler olarak: Paket veri değerlerini hex baytları olarak aktarır.

PSML XML olarak: Paketleri PSML (packet summary markup language) XML dosya formatında dışa aktarmaya yarar.

PDML XML olarak: Paketleri PDML (Packet Details Markup Language) XML dosyası olarak aktarmaya yarar.

Yazdır: Ctrl+P kısayol tuşlarıyla çalışır. Seçilen paketleri yazdırmaya yarar.

Çık: Ctrl+Q kısayol tuşlarıyla çalışır. Programdan çıkar.

3.9 DÜZENLE MENÜSÜ

Düzenle	Görünüm	Git	Yakala	Analiz	İstatistikler	Telefon	Ka
Kopyala							
Paket Bul...					Ctrl+F		
Sonrakini Bul					Ctrl+N		
Öncekini Bul					Ctrl+B		
Paket(ler)i İşaretle/İşaretini Kaldır					Ctrl+M		
Tüm Görüntülenenleri İşaretle					Ctrl+Shift+M		
Tüm Görüntülenenlerin İşaretini Kaldır					Ctrl+Alt+M		
Sonraki İşaret					Ctrl+Shift+N		
Önceki İşaret					Ctrl+Shift+B		
Paket(ler)i Yoksay/Yoksay					Ctrl+D		
Tüm Görüntülenenleri Yoksay					Ctrl+Shift+D		
Tüm Görüntülenenleri Yoksay					Ctrl+Alt+D		
Zaman Referansını Ayarla/Ayarlamayı Kaldır					Ctrl+T		
Tüm Zaman Referans Ayarlarını Kaldır					Ctrl+Alt+T		
Sonraki Zaman Referansı					Ctrl+Alt+N		
Önceki Zaman Referansı					Ctrl+Alt+B		
Zaman Kaydırması...					Ctrl+Shift+T		
Paket Yorumları							
Tüm Paket Yorumlarını Sil							
Yapılandırma Profilleri...					Ctrl+Shift+A		
Tercihler...					Ctrl+Shift+P		

Düz Metin Olarak	
CSV olarak	
YAML olarak	
Tüm Görünür Öğeler	Ctrl+Alt+Shift+A
Tüm Görünür Seçilmiş Ağaç Öğeleri	
Açıklama	Ctrl+Alt+Shift+D
Alan Adı	Ctrl+Alt+Shift+F
Değer	Ctrl+Alt+Shift+V
Filtre Olarak	Ctrl+Shift+C

Kopyala: Veri bölmesinden tıklanan değeri filtre ifadesi olarak kopyalar. İstenilen bölüm seçilerek sağ fare menüsünden de yapılabilir.

Paket Bul: Ctrl+F kısayol tuşlarıyla çalışır. Birçok kritere göre arama yapmanıza imkan sağlar. Display filter seçeneği seçiliyse Wireshark filtreleme kriterlerine göre arama yapar. Basit protokol taramalarından kuvvetli filtreleme ifadelerine kadar birçok türde etkin arama yapılabilir.

Sonrakini Bul: Ctrl+N kısayol tuşlarıyla çalışır. Belirlenen kriterde bir sonraki paketi bulur.

Öncekini Bul: Ctrl+B kısayol tuşlarıyla çalışır. Belirlenen kriterde bir önceki paketi bulur.

Paket(leri) İşaretle/İşaretini Kaldır: Ctrl+M kısayol tuşlarıyla çalışır. Seçilen paketi işaretler.

Sonraki İşaret: Shift+Ctrl+N kısayol tuşlarıyla çalışır. Bir sonraki işaretli paketi bulur.

Önceki İşaret: Shift+Ctrl+B kısayol tuşlarıyla çalışır. Bir önceki işaretli paketi bulur.

Zaman Referansını Ayarla/Ayarlamayı Kaldır: Ctrl+T kısayol tuşlarıyla çalışır. Seçilen paketi zaman referansı olarak alır ve sonraki paketlerde o pakete göre zaman değerleri alır.

Yapılandırma Profilleri: Shift+Ctrl+A kısayol tuşlarıyla çalışır. Profil ekle-sil işlemlerini yapar.

Tercihler: Shift+Ctrl+P kısayol tuşlarıyla çalışır. Programla ilgili ayarlamaların yapıldığı bölümdür.

3.10 GÖRÜNÜM MENÜSÜ

Görünüm menüsü Wireshark Programının görünümüyle ilgili ayarların yapıldığı kısımdır. Araç çubuklarının görüntülenmesi, sayfa boyutlandırması, adres çözümleme seçenekleri (renk ayarları gibi) bu kısımda bulunur.

The screenshot shows the 'View' menu in Wireshark. The main menu items are: Görünüm, Git, Yakala, Analiz, İstatistikler, Telefon, Kablosuz, Ar. The 'Görünüm' menu is expanded, showing the following options:

- ☒ Ana Araç Çubuğu
- ☒ Araç Çubuğunu Filtrele
- ☒ Durum Çubuğu
- Tam ekran (F11)
- ☒ Paket Listesi
- ☒ Paket Ayrıntıları
- ☒ Paket Bayt
- Paket Şeması
- Zaman Görüntüleme Biçimi
- Ad Çözümlemesi
- Yaklaş
- Alt Ağaçları Genişlet (Shift+Sağa)
- Alt Ağaçları Daralt (Shift+Sola)
- Tümünü Genişlet (Ctrl+Sağa)
- Tümünü Daralt (Ctrl+Sola)
- Paket Listesini Renklendir
- Renklendirme Kuralları...
- Konuşmayı Renklendir
- Düzeni Sıfırla (Ctrl+Shift+W)
- Sütunları Yeniden Boyutlandır (Ctrl+Shift+R)
- Dahili
- Paketi Yeni Pencerede Göster
- Dosya Biçimi/Yakalama Olarak Yeniden Yükle (Ctrl+Shift+F)
- Tekrar yükle (Ctrl+R)

Blue arrows point from the 'Görünüm' menu to the following sub-menus:

- Time and Date (Günün Tarihi ve Saati):** Ctrl+Alt+1 to Ctrl+Alt+8. Options include: Günün Tarihi ve Saati (01-01-1970 01:02:03.123456), Yıl, Yılın Günü ve Günün Saati (1970/001 01:02:03.123456), Günün Saati (01:02:03.123456), 1970-01-01'den Beri Saniye, Yakalama Başlangıcından Beri Saniyeler, Önceki Yakalanan Paketten Beri Saniye, Önceki Görüntülenen Paketten Beri Saniye, UTC Tarihi ve Günün Saati (1970-01-01 01:02:03.123456), UTC Yılı, Yılın Günü ve Günün Saati (1970/001 01:02:03.123456), UTC Günün Saati (01:02:03.123456).
- Automatic (Otomatik):** Saniye, Saniyenin onda biri, Saniyenin yüzde biri, Milisaniye, Mikrosaniye, Nanosaniye, Saniyeleri Saat ve Dakikalarla Göster.
- Çözümleme (Resolution):** Çözümleme Adı Düzenle, Fiziksel Adresleri Çözümle (checked), Ağ Adreslerini Çözümle, Taşıma Adreslerini Çözümle.
- Zoom (Yaklaş/Uzaklaş):** Yaklaş (Ctrl++), Uzaklaş (Ctrl+-), Normal Boyut (Ctrl+0).
- Konuşma Hash Tabloları (Conversation Hash Tables):** Tespit edici Tabloları, Desteklenen Protokoller.

Ana Araç Çubuğu: Ana araç çubuğunu gizler veya gösterir.

Ana Araç Çubuğunu Filtrele: Filtre araç çubuğunu gizler veya gösterir.

Durum Çubuğu: Durum çubuğunu gizler veya gösterir.

Paket Listesi: Paket listesi bölmesini gizler veya gösterir.

Paket Ayrıntıları: Paketlerin detaylarını ASCII kodunda gösteren bölgeyi ekler ya da kaldırır.

Paket Bayt: Data Window penceresini ekler ya da kaldırır.

Zaman Görüntüleme Biçimi: Paketler yakalanırken, her pakete zaman damgası eklenir. Bu zaman damgaları, yakalama dosyasına kaydedilecek, böylece daha sonra analiz edilmek üzere hazır olacaklar. Wireshark' a zaman damgalarını tarih ve saat formatında görüntülemesini söyler.

Kullanılabilir sunum biçimleri şunlardır:

Günün Tarih ve Saati: 1970-01-01 01:02:03.123456 Paketin yakalandığı günün mutlak tarihi ve saati

Günün Saati: 01:02:03.123456 Paketin yakalandığı günün mutlak saati

Yakalamanın Başlangıcından Beri Saniye: 123.123456 Yakalama dosyasının başlangıcına veya bu paketten önceki ilk “Zaman Referansına” göre zaman

Önceki Yakalanan Paketten Beri Saniye: 1.123456 Bir önceki yakalanan pakete göre süre

Önceki Görüntülenen Paketten Beri Saniye: 1.123456 Bir önceki görüntülenen pakete göre zaman

Dönemden Beri Saniye (1970-01-01): 1234567890.123456 Döneme göre zaman (1 Ocak 1970 gece yarısı UTC)

Kullanılabilir hassasiyetler (diğer bir deyişle, görüntülenen ondalık basamak sayısı):

Otomatik (yakalama dosyasından) Yüklenen yakalama dosyası biçiminin zaman damgası hassasiyeti kullanılacaktır (varsayılan).

Saniye, saniyenin onda biri, saniyenin yüzde, Milisaniyeler, Mikro saniye veya nano saniye zaman damgası hassas verilen ayara zorlanacak. Gerçekte mevcut hassasiyet daha küçükse, sıfırlar eklenir. Hassasiyet daha büyükse, kalan ondalık basamaklar kesilecektir.

Ad Çözümleme:

- Çözümlenen Adı Düzenle

Ad çözümlemesi, bazı sayısal adres değerlerini insan tarafından okunabilir bir biçime dönüştürmeye çalışır. Yapılacak çözümlüğe bağlı olarak bu dönüştürmeleri yapmanın iki

olası yolu vardır: sistem/ağ hizmetlerini çağırmak veya Wireshark' a özgü yapılandırma dosyalarından çözümlemek.

Ad Çözünürlüğü Dezavantajları

Wireshark ile çalışırken isim çözümlemesi paha biçilmez olabilir ve hatta sizi saatlerce çalışmadan kurtarabilir. Ne yazık ki, dezavantajları da var.

Ad çözümlemesi genellikle başarısız olabilir. Çözümenecek ad, istenen ad sunucuları tarafından bilinmiyor olabilir veya sunucular mevcut değil ve ad Wireshark'ın yapılandırma dosyalarında da bulunmuyor.

Çözümlenen adlar mevcut olmayabilir. Wireshark, DNS sunucuları, yakalama dosyasının kendisi (örneğin bir pcapng dosyası için) ve sisteminizdeki ve profil dizininizdeki ana bilgisayar dosyaları dahil olmak üzere çeşitli kaynaklardan ad çözümleme bilgilerini alır. Yakalama dosyasını daha sonra veya farklı bir makinede açarsanız, çözümlenen adlar kullanılamayabilir. Sonuç olarak, siz veya bir başkası belirli bir yakalama dosyasını her açtığında, değişen ortamlar nedeniyle biraz farklı görünebilir.

DNS, yakalama dosyanıza ek paketler ekleyebilir. Wireshark'ın DNS sorgularından ve yanıtlarından gelen ekstra trafik, gidermeye çalıştığınız sorunu veya sonraki analizleri etkiliyorsa, gözlemci etkisi ile karşılaşabilirsiniz.

Uzak bir bağlantı üzerinden yakalama yaparken de aynı şey olabilir, örneğin SSH veya RDP.

Çözümlenen DNS adları Wireshark tarafından önbellege alınır. Kabul edilebilir performans için bu gereklidir. Ancak, Wireshark çalışırken ad çözümleme bilgisinin değişmesi gerekiyorsa, Wireshark önbellege alındıktan sonra ad çözümleme bilgisinde bir değişiklik fark etmeyecektir. Bu bilgi Wireshark çalışırken değişirse, örneğin yeni bir DHCP kiralaması yürürlüğe girerse, Wireshark bunu fark etmeyecektir.

Paket listesinde isim çözümlemesi liste doldurulurken yapılır. Listeye bir paket eklendikten sonra bir ad çözülebilirse, önceki girişi değiştirilmez. Ad çözümleme sonuçları önbellege alınırken, paket listesini doğru çözümlenen adlarla yeniden oluşturmak için Görünüm/ Yeniden Yükle' yi kullanabilirsiniz. Ancak, bir yakalama devam ederken bu mümkün değildir.

Alt Ağaçları Genişlet: Paket ayrıntıları ağacında seçili olan alt ağacı genişletir.

Alt Ağaçları Daralt: Paket ayrıntıları ağacında hâlihazırda seçili olan alt ağacı daraltır.

Tümünü Genişlet: Wireshark, genişletilen tüm protokol alt ağaçlarının bir listesini tutar ve bir paketi görüntülediğinizde doğru alt ağaçların genişletilmesini sağlamak için bunu kullanır. Bu menü ögesi, yakalamadaki tüm paketlerdeki tüm alt ağaçları genişletir.

Tümünü Daralt: Yakalama listesindeki tüm paketlerin ağaç görünümünü daraltır.

Paket Listesini Renklendir: Wireshark'ın paket listesini renklendirmesi gerekip gerekmediğini kontrol etmenizi sağlar. Renklendirmeyi etkinleştirmek, yakalama dosyalarını yakalarken veya yüklerken yeni paketlerin görüntülenmesini yavaşlatacaktır.

Renklendirme Kuralları: Seçtiğiniz filtre ifadelerine göre paket listesi bölümündeki paketleri renklendirmenize izin veren bir iletişim kutusu açar. Belirli paket türlerini tespit etmek için çok faydalı olabilir

Konuşmayı Renklendir: Seçili paketin adreslerine göre paket listesi bölümündeki paketleri renklendirmenize izin veren bir alt menüyü getirir. Bu, farklı konuşmalara ait paketleri ayırt etmeyi kolaylaştırır.

Sütunları Yeniden Boyutlandır: İçeriğin içine sığması için tüm sütun genişliklerini yeniden boyutlandırın. Yeniden boyutlandırma, özellikle büyük bir yakalama dosyası yüklenmişse, önemli miktarda zaman alabilir.

Paketi Yeni Pencerede Göster: Seçili paketi ayrı bir pencerede gösterir. Ayrı pencere yalnızca paket ayrıntılarını ve baytları gösterir.

Tekrar Yükle: Geçerli yakalama dosyasını yeniden yüklemenizi sağlar.

3.11 GİT MENÜSÜ



Pakete Git: Ctrl+G kısayol tuşlarıyla çalışır. Paket numarasına göre istenilen pakete geçer.

Bağlantılı Pakete Git: Hali hazırda seçili protokol alanının ilgili paketine gidin. Seçilen alan bir pakete karşılık gelmiyorsa bu öge grileşir.

Sonraki Paket: Ctrl+aşağı kısayol tuşlarıyla çalışır. Seçili paketten sonraki pakete geçerler.

Önceki Paket: Ctrl+yukarı Seçili paketten önceki pakete geçer.

İlk Paket: Yakalanan ilk pakete geçer.

Son Paket: Yakalanan son pakete geçer.

Görüşmede Önceki Paket: Ctrl+, Geçerli konuşmada önceki pakete gidin. Bu, paket listesinde klavye odağı olmasa bile önceki pakete geçmek için kullanılabilir.

Görüşmedeki Sonraki Paket: Ctrl+. Geçerli konuşmada bir sonraki pakete geçin. Bu, paket listesinde klavye odağı olmasa bile önceki pakete geçmek için kullanılabilir.

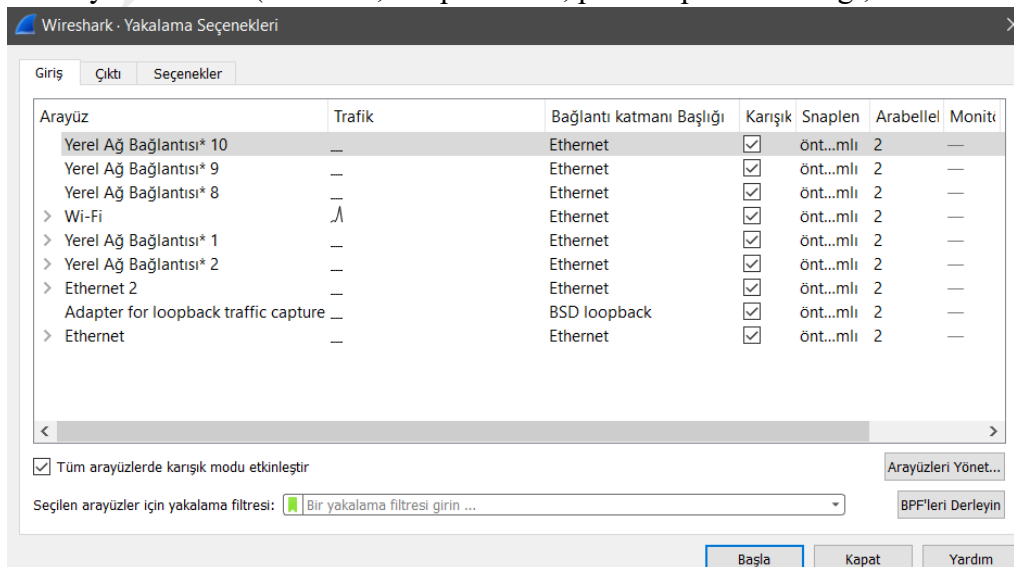
Geçmişteki Önceki Paket: Ctrl+sol kısayol tuşlarıyla çalışır. Bir önceki bakılan pakete geçer.

Geçmişteki Sonraki Paket: Ctrl+sağ kısayol tuşlarıyla çalışır. Ziyaret edilen bir sonraki pakete geçer.

3.12 YAKALA MENÜSÜ



Seçenekler: Uygulama sırasında kullanılacak ağ arabirimi seçimi, adres çözümleme özellikleri, görünüm özellikleri, uygulama durdurmak için ayarlanacak özellikler gibi birçok özellik ayarlanabilir. (IP adresi, tampon sınırı, paket toplama özelliği, filtreleme özelliği,



analiz
işlemini

kolaylaştırma, sistem kaynaklarını idareli kullanma, yakalanan paketleri eş zamanlı olarak anında ekranda görme, yakalanan paketlerin protokollere göre sayı ve oranını veren bilgi penceresinin saklaması, adres dönüşümü gibi birçok özellik bu kısımdadır.)

Başlat: Paket yakalama işlemini başlatır.

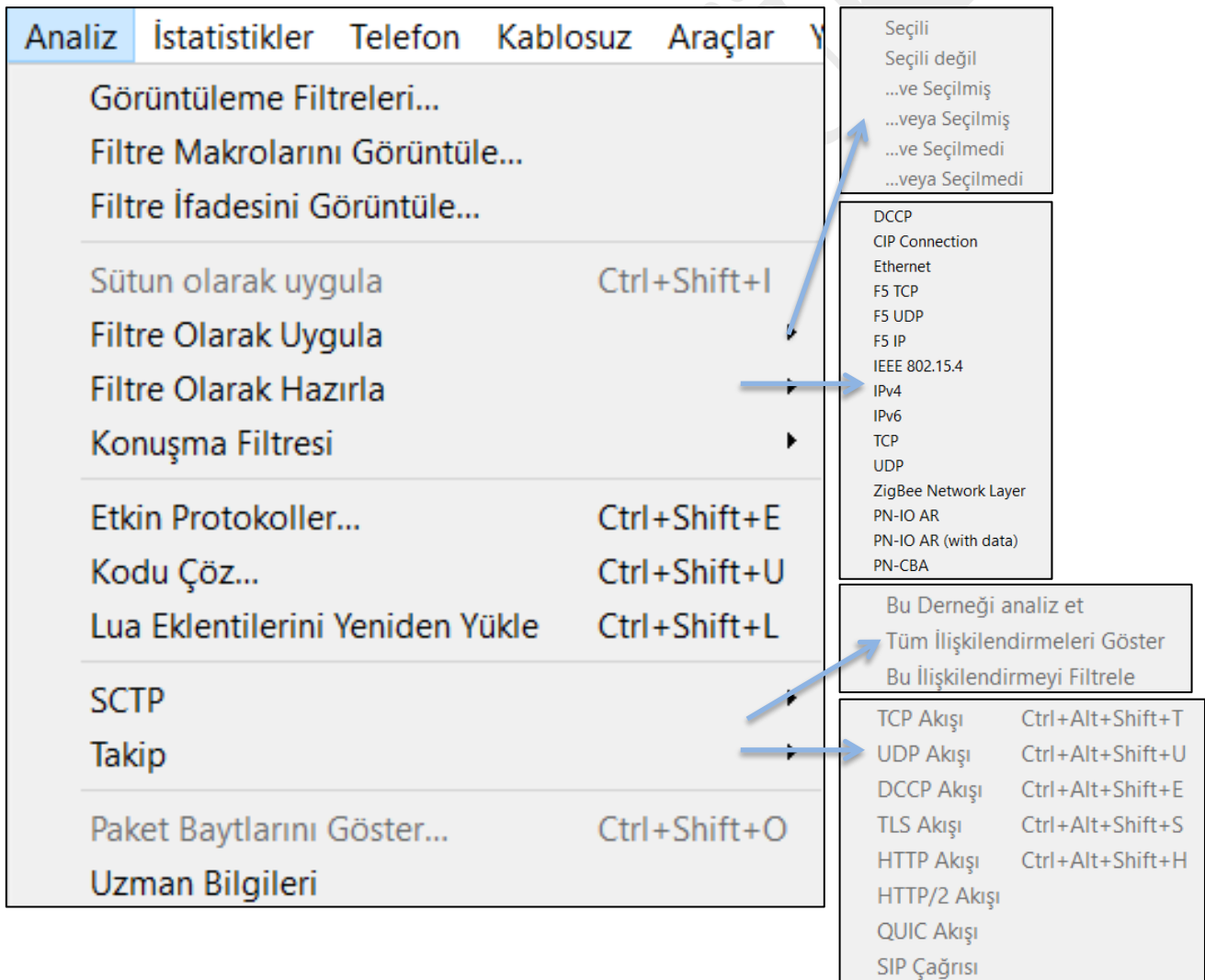
Durdur: Paket yakalama işlemini durdurur.

Yeniden Başlat: Ayarlanılan seçeneklere göre yakalama işlemini tekrar başlatır.

Yakalama Filtreleri: Paket yakalama işlemini ayarlanan filtrelere göre gerçekleştirir.

Arayüzleri Yenile: Wireshark' ın kullanacağı ağ arabirimi ve özellikleri yenilenir.

3.13 ANALİZ MENÜSÜ



Görüntüleme Filtreleri: Yakalanan paketleri belirtilen ifadelere göre sıralar.

Filtre Makrolarını Tanımlama ve Kaydetme: Wireshark ile bir filtre makrosu tanımlayabilir ve daha sonra kullanmak üzere etiketleyebilirsiniz. Bu, kullandığınız daha karmaşık filtrelerden bazılarını hatırlamak ve yeniden yazmak için zaman kazandırabilir.

Sütun Olarak Uygula: Paket ayrıntıları bölümünde seçili protokol ögesini paket listesine bir sütun olarak ekler.

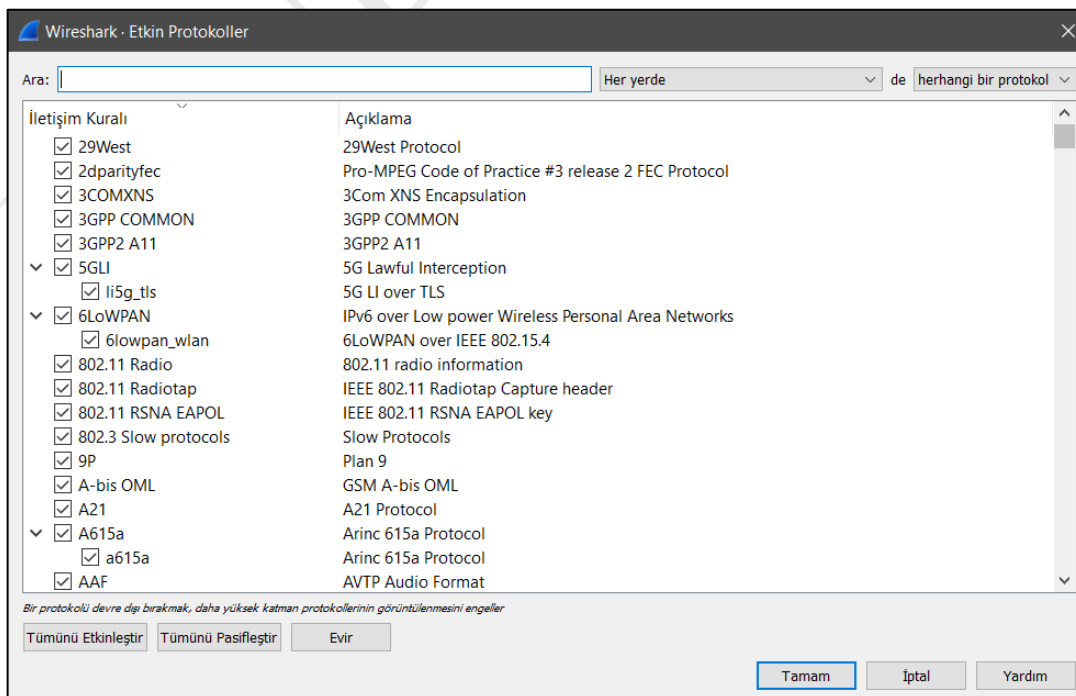
Filtre Olarak Uygula: Mevcut ekran filtresini değiştirin ve hemen uygulayın. Seçilen menü ögesine bağlı olarak, geçerli görüntü filtresi dizisi, paket ayrıntıları bölümünde seçilen protokol alanı tarafından değiştirilecek veya eklenecektir.

Filtre Olarak Hazırla: Geçerli görüntü filtresini değiştirin, ancak uygulamaz. Seçilen menü ögesine bağlı olarak, geçerli görüntü filtresi dizisi, paket ayrıntıları bölümünde seçilen protokol alanı tarafından değiştirilecek veya eklenecektir.

Konuşma Filtresi: Çeşitli protokoller için bir konuşma filtresi uygulayın.

"Etkin Protokoller" İletişim Kutusu: Etkin Protokoller iletişim kutusu, belirli protokolleri etkinleştirmenizi veya devre dışı bırakmanızı sağlar. Çoğu protokol varsayılan olarak etkindir. Bir protokol devre dışı bırakıldığında, Wireshark bu protokolle karşılaşıldığında bir paketi işlemeyi durdurur.

Not: Bir protokolü devre dışı bırakmak, daha yüksek katman protokolleri hakkındaki bilgilerin görüntülenmesini engeller. Örneğin, IP protokolünü devre dışı bıraktığınızı ve Ethernet, IP, TCP ve HTTP bilgilerini içeren bir paket seçtiğinizi varsayalım. Ethernet bilgileri görüntülenecektir, ancak IP, TCP ve HTTP bilgileri görüntülenmeyecektir - IP'nin devre dışı bırakılması, bunun ve daha yüksek katman protokollerinin görüntülenmesini engelleyecektir.



Bir protokolü devre dışı bırakmak veya etkinleştirmek için fareyi kullanarak onay kutusunu tıklamanız yeterlidir. Arama kutusuna protokol adının birkaç harfini yazmanın, listeyi bu harfleri içeren protokollerle sınırlayacağını unutmayın.

Aşağıdaki eylemler arasından seçim yapabilirsiniz:

- Hepsini etkinleştir: Listedeki tüm protokolleri etkinleştirin.
- Hepsini etkisiz hale getir: Listedeki tüm protokolleri devre dışı bırakın.
- Ters çevir: Listedeki tüm protokollerin durumunu değiştirin.
- Tamam: Değişiklikleri kaydedip uygulayın ve iletişim kutusunu kapatın, ayrıntılar için Dosyalar ve Klasörler' e bakın.
- İptal etmek: Değişiklikleri iptal edin ve iletişim kutusunu kapatın.

Uzman Bilgi: İletişimde meydana gelen olayların kaydeder. Yakalanan paketleri hatalar, notlar, uyarılar, konuşmalar şeklinde kriterlerine göre ayırır.

3.14 İSTATİSTİKLER MENÜSÜ

İstatistikler	Telefon	Kablosuz	Araçlar	Yardım
Yakalama Dosyası Özellikleri				Ctrl+Alt+Shift+C
Çözümlenen Adresler				
Protokol Hiyerarşisi				
Konuşmalar				
Uç Noktalar				
Paket Uzunlukları				
G/Ç Grafikleri				
Servis Yanıt Süresi				
DHCP (BOOTP) Statistics				
NetPerfMeter Statistics				
ONC-RPC Programs				
29Batı				
ANCP				
BACnet				
Toplanan				
DNS				
Akış Grafiği				
HART-IP				
HPFEEDS				
HTTP				
HTTP2				
Aynı zamanda				
TCP Akış Grafikleri				
UDP Çok Noktaya Yayın Akışları				
Güvenilir Sunucu Havuzu (RSerPool)				
F5				
IPv4 Statistics				
IPv6 Statistics				

Konular	Konuya Göre Reklamlar
Kuyruklar	Kaynağa Göre Reklamlar
UIM	Ulaşım Reklamları
LBT-RM	Konuya Göre Sorgular
LBT-RU	Alıcıya Göre Sorgular
	Desene Göre Joker Karakter Sorguları
	Alıcıya Göre Joker Karakter Sorguları

Örnek Kimliğine göre sıralanmış paketler
IP'ye göre sıralanmış paketler
Nesne türüne göre sıralanmış paketler
Servise göre sıralanmış paketler

Paket Sayacı
İstekler
Yük Dağılımı
İstek Dizileri

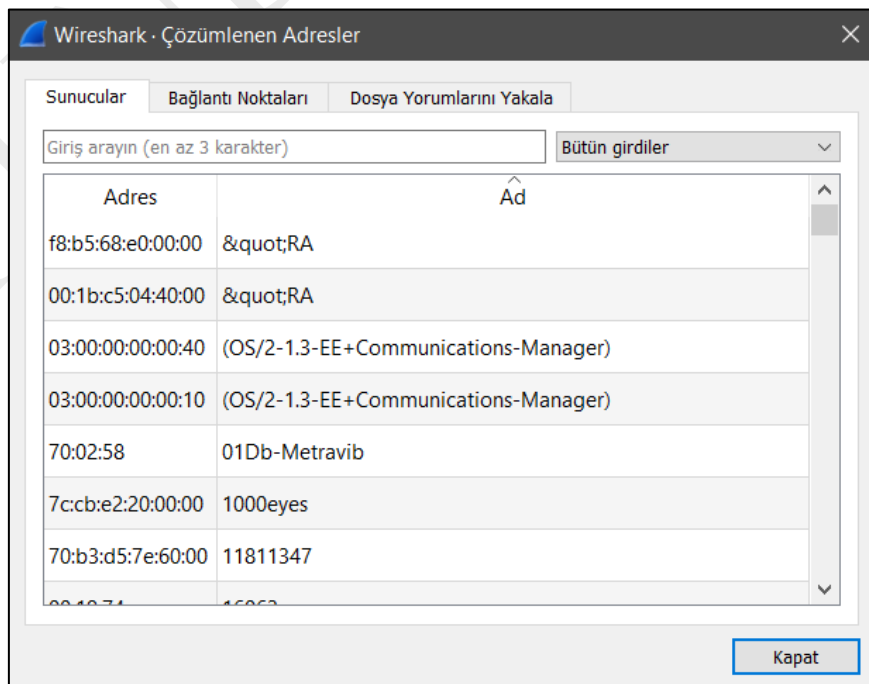
Zaman Dizisi (Stevens)
Zaman Sırası (tcptrace)
Verim
Gidiş-dönüş süresi
Pencere Ölçekleme

All Addresses
Destinations and Ports
IP Protocol Types
Source and Destination Addresses

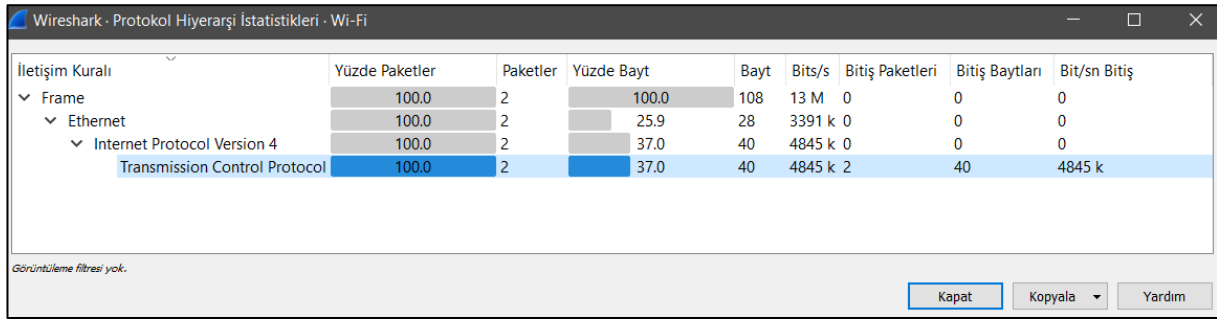
Yakalama Dosyası Özellikleri: Geçerli yakalama dosyası hakkında genel bilgiler verir. Bu iletişim kutusu şu bilgileri gösterir;

- Detaylar: Yakalama dosyası hakkında önemli bilgiler,
- Dosya: Tam yolu, boyutu, şifreleme karmaları, dosya biçimi ve kapsülleme dâhil, yakalama dosyası hakkında genel bilgiler,
- Zaman: Dosyadaki ilk ve son paketin zaman damgaları ve farklarını,
- Ele geçirmek: Yakalama ortamı hakkında bilgi. Bu, yalnızca canlı yakalamalar için veya bu bilgiler kaydedilmiş bir yakalama dosyasında mevcutsa gösterilecektir. pcapng formatı bunu desteklerken pcap desteklemez.
- Arayüzler: Yakalama arabirimi veya arabirimleri hakkında bilgi.
- İstatistik: Yakalama dosyasının istatistiksel bir özeti. Bir görüntüleme filtresi ayarlanmışsa, Yakalanan sütununda değerler göreceksiniz ve herhangi bir paket işaretlenmişse, İşaretli sütununda değerler göreceksiniz. Yakalanan sütunundaki değerler öncekiyle aynı kalacak, Görüntülenen sütunundaki değerler ise ekranda gösterilen paketlere karşılık gelen değerleri yansıtacaktır. Değerler İşaretli sütuna işaretlenmiş paketlere karşılık gelen değerlerini yansıtır.
- Dosya yorumlarını yakala: Bazı yakalama dosyası biçimleri (özellikle pcapng), tüm dosya için bir metin yorumuna izin verir. Bu yorumu buradan görüntüleyebilir ve düzenleyebilirsiniz.

Çözümlenen Adresler: Çözümlenen adreslerin listesini ve ana bilgisayar adlarını gösterir. Kullanıcılar, Hosts yalnızca IPv4 ve IPv6 adreslerini görüntülemek için alanı seçebilir . Bu durumda, iletişim kutusu, bilinen bir ana bilgisayara sahip bir yakalama dosyasındaki her IP adresi için ana bilgisayar adlarını görüntüler. Bu ana bilgisayar genellikle bir yakalama dosyasındaki DNS yanıtlarından alınır. Bilinmeyen bir ana bilgisayar adı olması durumunda, kullanıcılar bunu ters DNS aramasına göre doldurabilir.



Protokol Hiyerarşisi: Yakalanan paketlerin protokol hiyerarşisini gösterir.



İletişim Kuralı	Yüzde Paketler	Paketler	Yüzde Bayt	Bayt	Bits/s	Bitiş Paketleri	Bitiş Baytları	Bit/sn Bitiş
Frame	100.0	2	100.0	108	13 M	0	0	0
Ethernet	100.0	2	25.9	28	3391 k	0	0	0
Internet Protocol Version 4	100.0	2	37.0	40	4845 k	0	0	0
Transmission Control Protocol	100.0	2	37.0	40	4845 k	2	40	4845 k

Görüntüleme filtresi yok.

Kapat Kopyala Yardım

Bu, yakalamadaki tüm protokollerin bir ağacıdır. Her satır, bir protokolün istatistiksel değerlerini içerir. Sütunlardan ikisi (Paket Yüzdesi ve Bayt Yüzdesi) çubuk grafikler olarak çifte görev yapar. Bir ekran filtresi ayarlanmışsa, altta gösterilecektir.

Kopya düğmesi CSV ya YAML olarak pencere içeriğini kopyalamak izin verir.

Protokol hiyerarşisi sütunları ve görevleri şu şekildedir;

- Protokol: Bu protokolün adını gösterir.
- Yüzde Paketler: Yakalamadaki tüm paketlere göre protokol paketlerinin yüzdesini gösterir.
- Paketler: Bu protokolün toplam paket sayısı.
- Yüzde Bayt: Yakalamadaki toplam baytlara göre protokol baytlarının yüzdesi.
- Bayt: Bu protokolün toplam bayt sayısını gösterir.
- Bits/s: Yakalama süresine göre bu protokolün bant genişliği.
- Bitiş Paketleri: Yığındaki en yüksek protokol olduğu (son incelenen) bu protokolün mutlak paket sayısı.
- Bitiş Baytları: Yığındaki (son incelenen) en yüksek protokol olduğu yerde bu protokolün mutlak bayt sayısını gösterir.
- Bit/sn Bitiş: Bu protokolün, yığındaki en yüksek protokolün olduğu (son incelenen) yakalama süresine göre bant genişliği.

Paketler genellikle birden çok protokol içerir. Sonuç olarak, her paket için birden fazla protokol sayılacaktır. Örnek: Ekran görüntüsünde IP'nin %99,9'u ve TCP'nin %98,5'i (birlikte %100'den çok daha fazladır).

Protokol katmanları, herhangi bir üst katman protokolü içermeyen paketlerden oluşabilir, bu nedenle tüm yüksek katman paketlerinin toplamı protokol paket sayısına eşit olmayabilir. Örnek: Ekran görüntüsünde TCP %98,5'e sahiptir ancak alt protokollerin (TLS, HTTP, vb.) toplamı çok daha azdır. Bu, devam çerçeveleri, TCP protokolü ek yükü ve diğer kesilmemiş verilerden kaynaklanabilir.

Tek bir paket aynı protokolü birden fazla içerebilir. Bu durumda, protokol bir kereden fazla sayılır. Örneğin ICMP yanıtları ve birçok tünel protokolü birden fazla IP başlığı taşıyacaktır.

Konuşmalar: Bir ağ konuşması, iki belirli uç nokta arasındaki trafiktir. Adresler, paket sayacıları ve bayt sayacılarının yanı sıra konuşma penceresi dört sütun ekler: konuşmanın

başlangıç zamanı ("Rel Start") veya ("Mutlak Başlangıç"), konuşmanın saniye cinsinden süresi ve ortalama bitler (bayt değil) her yönde saniyede. "Rel Start" / "Abs Start" ve "Süre" sütunları boyunca bir zaman çizelgesi grafiği de çizilir.

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
48:5f:99:31:b8:5b	01:00:5e:7f:ff:fa	4	864	4	864	0	0	0 41.491928	3.0387	2274	0
84:b5:41:f8:fc:f0	48:5f:99:31:b8:5b	20	3210	20	3210	0	0	0 30.483980	8.6249	2977	0
9c:69:d1:2b:e5:fc	ff:ff:ff:ff:ff:ff	25	1050	25	1050	0	0	0 2.732476	42.0870	199	0
9c:69:d1:2b:e5:fc	48:5f:99:31:b8:5b	14	782	7	402	7	380	4.990725	34.1184	94	89
b4:f6:1ca0:b4:49	48:5f:99:31:b8:5b	15	2313	15	2313	0	0	0 0.000000	31.0022	596	0
bc:30:7d:cb:b0:1b	ff:ff:ff:ff:ff:ff	1	42	1	42	0	0	0 30.688203	0.0000	—	0
bc:30:7d:cb:b0:1b	48:5f:99:31:b8:5b	4	1344	4	1344	0	0	0 41.512311	3.0399	3537	0

Listedeki her satır, tam olarak bir görüşme için istatistiksel değerleri gösterir. Pencerede seçilirse ve belirli protokol katmanını için etkinse (seçilen Ethernet uç noktaları sayfası için MAC katmanı) ad çözümlemesi yapılacaktır. Görüntüleme filtresiyle sınırla , yalnızca geçerli görüntüleme filtresiyle eşleşen konuşmaları gösterir. Mutlak başlangıç zamanı , başlangıç zamanı sütununu görelili ("Rel Start") ve mutlak ("Mutlak Başlangıç") zamanlar arasında değiştirir. Göreceli başlangıç zamanları, paket listesindeki "Yakalamanın Başından Bu yana Saniye" zaman görüntüleme biçimiyle ve mutlak başlangıç zamanları "Günün Zamanı" görüntüleme biçimiyle eşleşir.

Kopya düğmesi CSV panoya (virgülle ayrılmış değerler) veya YAML biçimine liste değerlerini kopyalar.

Uç Noktalar: Bir özellik arıyorsanız, diğer ağ araçları bir ana bilgisayar listesi çağırır, bakmak için doğru yer burasıdır. Ethernet veya IP uç noktalarının listesi genellikle aradığınız şeydir. Yakalanan uç noktalarla ilgili istatistikleri gösterir.

(Uç Nokta ve Konuşma türleri: Ethernet, Bluetooth, fiber Kanal, IEEE 802.11, FDDI, FDDI MAC-48, IPv4, IPv6, IPX, JXTA, NCP, SCTP, TCP, jeton yüzük, UDP, USB)

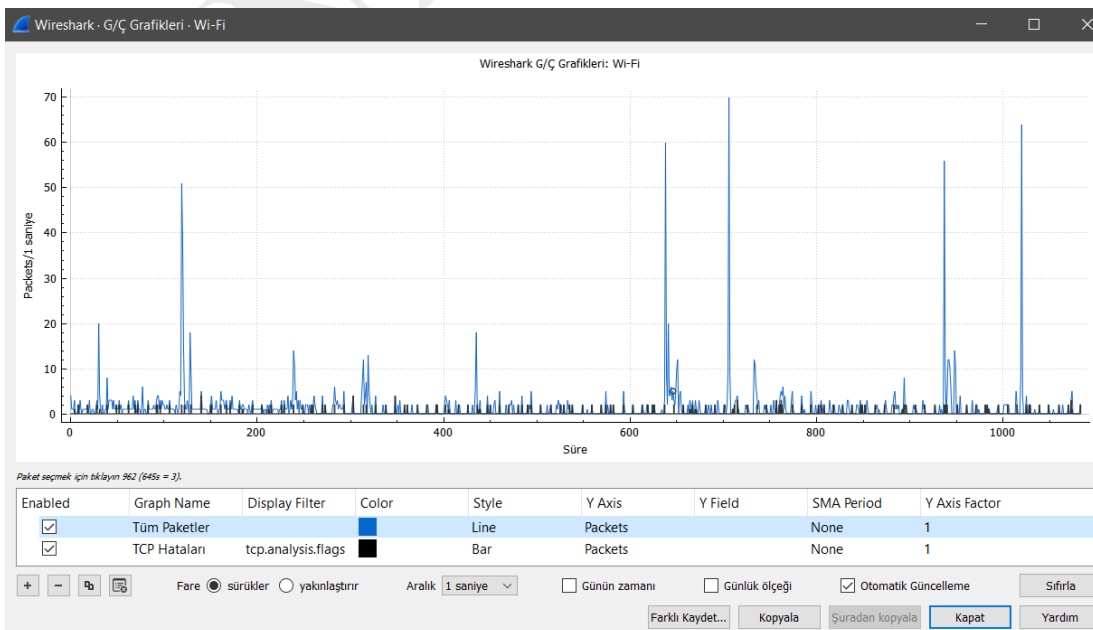
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:00:5e:7f:ff:fa	16	3456	0	0	16	3456
48:5f:99:31:b8:5b	571	151 k	175	39 k	396	112 k
84:b5:41:f8:fc:f0	47	7463	47	7463	0	0
88:46:04:68:68:95	64	27 k	64	27 k	0	0
9c:69:d1:2b:e5:fc	522	86 k	367	50 k	155	35 k
b4:f6:1ca0:b4:49	38	5689	38	5689	0	0
bc:30:7d:cb:b0:1b	40	12 k	36	12 k	4	168
e8:5a:8b:36:ca:ff	48	17 k	48	17 k	0	0
ff:ff:ff:ff:ff:ff	204	9176	0	0	204	9176

Desteklenen her protokol için bu pencerede bir sekme gösterilir. Her sekme etiketi yakalanan uç noktaların sayısını gösterir. Belirli bir protokolün hiçbir uç noktası yakalanmadıysa, sekme etiketi grileşir. Listedeki her satır, tam olarak bir uç nokta için istatistiksel değerleri gösterir. Pencerede seçilirse ve belirli protokol katmanı için etkinse ad çözümlemesi yapılacaktır. Görüntüleme filtresiyle sınırla, yalnızca geçerli görüntüleme filtresiyle eşleşen konuşmaları gösterir.

Paket Uzunlukları: Paket uzunluklarının ve ilgili bilgilerin dağılımını gösterir.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
✓ Packet Lengths	1029	217,48	42	1292	0,0015	100%	0,3200	119,777
0-19	0	-	-	-	0,0000	0,00%	-	-
20-39	0	-	-	-	0,0000	0,00%	-	-
40-79	549	53,58	42	79	0,0008	53,35%	0,1400	120,085
80-159	126	117,56	80	155	0,0002	12,24%	0,0700	119,779
160-319	159	195,75	161	305	0,0002	15,45%	0,1700	30,483
320-639	83	403,88	334	602	0,0001	8,07%	0,0300	641,153
640-1279	64	827,14	664	1132	0,0001	6,22%	0,0600	120,003
1280-2559	48	1291,25	1288	1292	0,0001	4,66%	0,1200	119,778
2560-5119	0	-	-	-	0,0000	0,00%	-	-
5120 and greater	0	-	-	-	0,0000	0,00%	-	-

G/Ç Grafikleri: Paket ve protokol verilerini çeşitli şekillerde çizmenizi sağlar.



Grafikler mevcut profilinize kaydedilir. Aşağıda açıklandığı gibi ayarlanabilen zaman aralıklarına bölünmüşlerdir. Grafiğin üzerine gelindiğinde, aşağıda belirtilenler dışında her aralıktaki son paket gösterilir. Grafiğe tıklamak sizi paket listesindeki ilgili pakete götürür. Bireysel grafikler aşağıdaki seçenekler kullanılarak yapılandırılabilir:

- Etkinleştirilmiş: Bu grafiği çizin veya çizmeyin.
- Grafik Adı: Bu grafiğin adıdır.
- Ekran Filtresi: Grafiği, bu filtreyle eşleşen paketlerle sınırlar.
- Renk: Grafiğin çizgilerini, çubuklarını veya noktalarını çizmek için kullanılacak renk.
- Stil: Grafik verilerinin görsel olarak nasıl temsil edileceği, örneğin bir çizgi, çubuk, daire, artı vb. çizer.
- Y eksenini Grafiğin Y eksenini için kullanılacak değer. Şunlardan biri olabilir:
- Paketler, Baytlar veya Bitler: Aralık başına grafiğin görüntüleme filtresiyle eşleşen toplam paket, paket bayt veya paket bit sayısı. Bazı durumlarda sıfır değerler atlanır.
- SUM(Y Alanı): Aralık başına “Y Alanı” nda belirtilen alanın değerlerinin toplamı.
- SAYISI ÇERÇEVE(Y Alanı): Aralık başına “Y Alanı” nda belirtilen alanı içeren çerçeve sayısı. Düz “Paketler” grafiğinden farklı olarak, bu her zaman sıfır değerleri görüntüler.
- COUNT ALAN(Y Alanı): Aralık başına “Y Alanı” nda belirtilen alanın örnek sayısı. dns.resp.name gibi bazı alanlar bir pakette birden çok kez görünebilir .
- MAX(Y Alanı), MIN(Y Alanı), AVG(Y Alanı): Aralık başına belirtilen “Y Alanı” nın maksimum, minimum ve aritmetik ortalama değerleri. MAX ve MIN değerleri için grafiğin üzerine gelip tıklamak sizi en son paket yerine aralıkta MAX veya MIN değeri olan pakete götürecektir.
- YÜK(Y Alanı): "Y Alanı" göreceli bir zaman değeriye, “Y Alanı” değerlerinin toplamının aralık süresine bölümüdür. Bu, yanıt sürelerini izlemek için yararlı olabilir.
- Y Alanı: Yukarıda listelenen Y eksenini hesaplamaları için değerlerin çıkarılacağı ekran filtresi alanı.
- SMA Dönemi: Belirli bir aralıktaki değerlerin ortalamasını gösterin.
- Bir bütün olarak çizelge, grafik listesi altındaki kontroller kullanılarak yapılandırılabilir:
- +: Yeni bir grafik ekleyin.
- -: Yeni bir grafik ekleyin.
- Kopyala: Seçilen grafiği kopyalayın.
- Temizlemek: Tüm grafikleri kaldırın.
- Fare sürükler / yakınlaştırır: Fareyi grafik alanı içinde kullanırken, grafik içeriğini sürükleyin veya bir yakınlaştırma alanı seçin.
- Aralık: Grafik için aralık periyodunu ayarlayın.
- Günün zamanı: X ekseninde günün mutlak saatini veya yakalama başlangıcından itibaren göreceli saati gösterme arasında geçiş yapın.
- Günlük ölçeği: Logaritmik veya doğrusal Y eksenini arasında geçiş yapın.

Wireshark 'ın G/Ç Grafiği penceresi eksik ve sıfır değerler arasında ayırım yapmaz. Dağılım grafikleri için sıfır değerlerinin eksik verileri gösterdiği varsayılır ve bu değerler atlanır. Sıfır değerleri çizgi grafiklerde ve çubuk grafiklerde gösterilir.

Servis Yanıt Süresi: Çeşitli yanıt süresi istatistikleriyle birlikte yakalama dosyasında bulunan her SMB2 işlem kodu için işlem sayısını gösterir. Bir satıra sağ tıklamak, belirli bir işlem kodu için filtreler uygulamanıza veya hazırlamanıza, aramanıza veya renklendirmenize olanak tanır. Ayrıca tüm yanıt süresi bilgilerini kopyalayabilir veya çeşitli biçimlerde kaydedebilirsiniz.

DHCP (BOOT) Statistics: Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP), Önyükleme Protokolü'nün (BOOTP) bir seçeneğidir. IP adreslerini ve diğer parametreleri bir DHCP istemcisine dinamik olarak atar. DHCP (BOOTP) İstatistikleri penceresi, bir DHCP mesaj türünün oluşum sayısı üzerinden bir tablo görüntüler. Kullanıcı verileri filtreleyebilir, kopyalayabilir veya bir dosyaya kaydedebilir.

NetPerfMeter Statistics: NetPerfMeter Protokolü (NPMP), aktarım protokolü performans test aracı olan NetPerfMeter'in kontrol ve veri aktarım protokolüdür. Veri akışlarını, kare hızı, kare boyutu, doymuş akışlar vb. gibi belirli parametrelerle TCP, SCTP, UDP ve DCCP üzerinden iletir. Bu istatistikle şunları yapabilirsiniz:

- Mesaj tipi başına gözlemlenen mesaj ve bayt sayısı,
- Her mesaj türü için mesajların ve baytların payı,
- Her mesaj türünün ilk ve son oluşumunu görün,
- Her mesaj türünün ilk ve son tekrarı arasındaki aralığa bakın (karşılık gelen türden en az 2 mesaj varsa),
- Her mesaj türü için aralık içindeki mesaj ve bayt hızına bakın (karşılık gelen türden en az 2 mesaj varsa).

ONC-RPC Programları: Açık Ağ Bilgi İşlem (ONC) Uzaktan Yordam Çağrısı (RPC), bir program numarasını uzak bir makinedeki belirli bir bağlantı noktasına eşlemek ve bu bağlantı noktasında gerekli bir hizmeti aramak için TCP veya UDP protokollerini kullanır. ONC-RPC Programları penceresi, program adı, numarası, sürümü ve diğer veriler gibi yakalanan program çağrılarının açıklamasını gösterir.

29Batı: 29West teknolojisi artık Ultra Düşük Gecikmeli Mesajlaşma (ULLM) teknolojisini ifade ediyor. Sıfır gecikmeli veri teslimi için mikro saniye teslim süreleriyle saniyede yüksek sayıda mesaj göndermeye ve almaya izin verir.

İstatistik / 29West gösterileri:

Konular menü şu sayaçları gösterir:

- Konuya Göre Reklam
- Kaynağa Göre Reklam
- Ulaşım Reklamı
- Konuya Göre Sorgular
- Alıcıya Göre Sorgular
- Desene Göre Joker Karakter Sorguları
- Alıcıya Göre Joker Karakter Sorguları

Kuyruklar menü şu sayaçları gösterir:

- Sıraya Göre Reklam
- Kaynağa Göre Reklam
- Kuyruğa Göre Sorgular
- Alıcıya Göre Sorgular

UIM menü için şunları gösterir:

Her akış, Bitiş Noktaları, Mesajlar, Baytlar ve İlk ve Son Çerçeve istatistikleri tarafından sağlanır.

LBT-RM menü için şunları gösterir:

LBT-RM Aktarım İstatistikleri penceresi, aktarım ve diğer veriler için Kaynaklar ve Alıcılar sıra numaralarını gösterir.

LBT-RU menü şunları gösterir:

LBT-Ru Taşıma İstatistikleri penceresi, aktarım ve diğer veriler için Kaynaklar ve Alıcılar sıra numaralarını gösterir.

ANCP: Erişim Düğümü Kontrol Protokolü (ANCP), bir Erişim Düğümü ile Ağ Erişim Sunucusu arasında çalışan TCP tabanlı bir protokoldür. Wireshark ANCP ayrıştırıcısı, aşağıda listelenen mesajları destekler:

- Bitişik Mesaj
- Port-Up ve Port-Down Mesajları gibi Topoloji Keşfi Uzantıları
- Port Yönetim Mesajı gibi İşletme ve Bakım (OAM) Uzantısı.
- ANCP penceresi ilgili istatistiksel verileri gösterir. Kullanıcı verileri filtreleyebilir, kopyalayabilir veya bir dosyaya kaydedebilir.

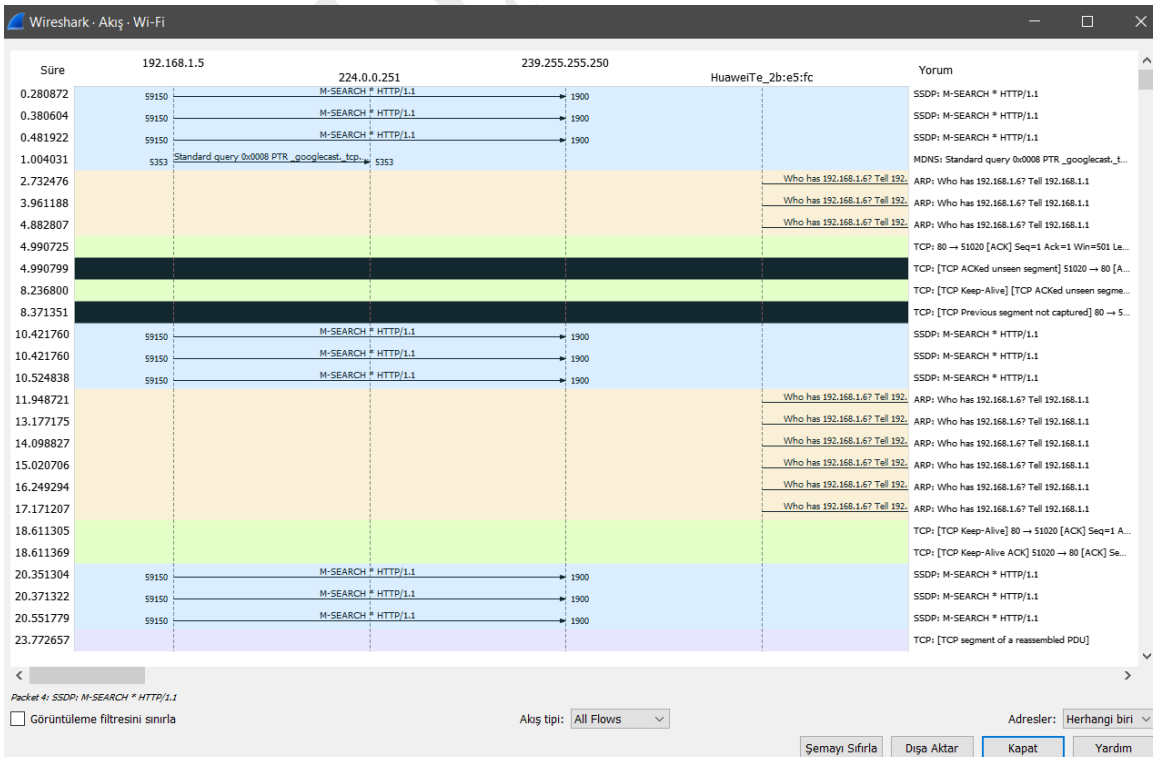
BACnet: Bina Otomasyon ve Kontrol Ağları (BACnet), ısı kontrolü, yangın alarmı kontrolü ve diğerleri gibi çeşitli bina otomasyonu tesisleri için kontrol sağlayan bir iletişim protokolüdür. Wireshark, bir paket sayacı olan BACnet istatistiklerini sağlar. Paketleri örnek kimliğine, IP adresine, nesne türüne veya hizmete göre sıralayabilirsiniz.

Toplanan: Bir sistem istatistikleri toplama arka plan programıdır. Sisteminizden çeşitli istatistikler toplar ve ağ kullanımı için dönüştürür. Toplanan istatistikler penceresi, toplam paket sayacının yanı sıra tür, eklenti ve ana bilgisayar olarak ayrılan değerler için sayıları gösterir. Verileri filtreleyebilir, kopyalayabilir veya bir dosyaya kaydedebilirsiniz.

DNS: Alan Adı Sistemi (DNS), IP adresleri gibi farklı bilgileri alan adlarıyla ilişkilendirir. DNS, çeşitli toplamalar için farklı kodlar, istek-yanıt ve sayaçlar döndürür. DNS istatistikleri penceresi, istek türlerine (işlem kodları), yanıt koduna (rcode), sorgu türüne ve diğerlerine göre gruplara ayrılan toplam DNS iletisi sayısını listeler.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
▼ Total Packets	130				0,0001	100%	0,0600	1829,073
▼ rcode	130				0,0001	100,00%	0,0600	1829,073
No error	130				0,0001	100,00%	0,0600	1829,073
▼ opcodes	130				0,0001	100,00%	0,0600	1829,073
Standard query	130				0,0001	100,00%	0,0600	1829,073
▼ Query/Response	130				0,0001	100,00%	0,0600	1829,073
Response	65				0,0000	50,00%	0,0400	1829,082
Query	65				0,0000	50,00%	0,0200	637,935
▼ Query Type	130				0,0001	100,00%	0,0600	1829,073
AAAA (IPv6 Address)	12				0,0000	9,23%	0,0300	1829,073
A (Host Address)	118				0,0001	90,77%	0,0400	638,030
▼ Class	130				0,0001	100,00%	0,0600	1829,073
IN	130				0,0001	100,00%	0,0600	1829,073
▼ Service Stats	0				0,0000	100%	-	-
request-response time (msec)	39	107,86	6,713000	494,984009	0,0000		0,0200	1681,570
no. of unsolicited responses	0				0,0000		-	-
no. of retransmissions	26				0,0000		0,0200	1829,088
▼ Response Stats	0				0,0000	100%	-	-
no. of questions	130	1,00	1	1	0,0001		0,0800	1829,082
no. of authorities	130	4,37	2	8	0,0001		0,0800	1829,082
no. of answers	130	1,86	1	5	0,0001		0,0800	1829,082
no. of additionals	130	8,18	5	12	0,0001		0,0800	1829,082

Akış Grafiği: Akış Grafiği penceresi, ana bilgisayarlar arasındaki bağlantıları gösterir. Yakalanan her bağlantı için paket zamanını, yönünü, bağlantı noktalarını ve yorumları görüntüler. Tüm bağlantıları ICMP Akışları, ICMPv6 Akışları, UIM Akışları ve TCP Akışları ile filtreleyebilirsiniz. Akış Grafiği penceresi, birden fazla farklı konuyu göstermek için kullanılır. Buna dayanarak, farklı kontroller sunar.



Her dikey çizgi, pencerenin üst kısmında görebileceğiniz belirli ana bilgisayarı temsil eder.

Pencerenin en solundaki her satırdaki sayılar zaman paketini temsil eder. Saat biçimini Görünüm /Saat Görüntüleme Biçimi' nde değiştirebilirsiniz. Saat biçimini değiştirirseniz, saati yeni bir biçimde gözlemlemek için Akış Grafiği penceresini yeniden başlatmanız gerekir.

Ana bilgisayarlar arasındaki her bir okun her iki ucundaki sayılar, bağlantı noktası numaralarını temsil eder.

Paket listesinde ilgili paketi seçmek için bir satıra sol tıklayın. Paket listesinde önceki, mevcut veya sonraki paketi seçme gibi ek seçenekler için grafiğe sağ tıklayın. Bu menü ayrıca diyagramı taşımak için kısayollar içerir.

Mevcut kontroller:

- Filtre filtre çağrılarını yalnızca görüntüleme filtresiyle eşleşenlerle sınırla. Pencere açılmadan görüntü filtresi aktif olduğunda onay kutusu işaretlenir.
- Akış tipi, protokol akışlarının limit tipine dayandırılmasına izin verir.
- Adresler, şemada gösterilen adreslerin değiştirilmesine izin verir.
- Diyagramı Sıfırla, görünüm konumunu sıfırlar ve varsayılan duruma yakınlaştırır.
- Dışa aktarma, diyagramı birden çok farklı formatta (PDF, PNG, BMP, JPEG ve ASCII (diyagram yalnızca ASCII karakterleriyle saklanır) görüntü olarak dışa aktarmaya izin verir).

HART-IP: IP üzerinden Otoyol Adreslenebilir Uzak Dönüştürücü (HART-IP), bir uygulama katmanı protokolüdür. Akıllı cihazlar ile kontrol veya izleme sistemleri arasında dijital bilgi gönderir ve alır. HART-IP istatistik penceresi, yanıt, istek, yayınlama ve hata paketleri için sayacı gösterir. Verileri filtreleyebilir, kopyalayabilir veya bir dosyaya kaydedebilirsiniz.

HPFEED'LER: Hpfeeds protokolü, hafif, kimliği doğrulanmış bir yayınlama ve abonelik sağlar. Farklı kanallara ayrılabilen isteğe bağlı ikili yükleri destekler. HPFEEDS istatistik penceresi, kanal ve işlem kodları başına yük boyutu için bir sayaç gösterir. Verileri filtreleyebilir, kopyalayabilir veya bir dosyaya kaydedebilirsiniz.

HTTP2: Köprü Metni Aktarım Protokolü sürüm 2 (HTTP/2), çeşitli HTTP isteklerinin ve yanıtlarının tek bir bağlantı üzerinden çoğullaşmasına olanak tanır. Çerçevelerden oluşan ikili bir kodlama kullanır. HTTP / 2 istatistik pencere Şekil HTTP toplam sayısı / 2 gibi, aynı zamanda çerçeve türleri başına dökümünü sağlar ve çerçeveler, HEADERS, DATA ve diğerleri. HTTP/2 trafiği tipik olarak TLS ile şifrelendiğinden, HTTP/2 trafiğini gözlemlemek için şifre çözme yapılandırmanız gerekir.

Aynı Zamanda: Sametime, IBM Sametime yazılımı için bir protokoldür. Sametime istatistik penceresi, mesaj türü, gönderme türü ve kullanıcı durumu için sayacı gösterir.

TCP Akış Grafikleri: Bir yakalamada TCP akışlarının farklı görsel temsillerini gösterin.

- Zaman Dizisi (Stevens) menüsü

Bu, Richard Stevens'in “TCP/IP Illustrated” kitaplarında kullanılanlara benzer, zaman içindeki TCP sıra numarasının basit bir grafiğidir.

- Zaman Sırası (tcptrace) menüsü

İletim kesimleri, bildirimler, seçici onaylar, ters pencere boyutları ve sıfır pencereleri dahil olmak üzere tcptrace yardımcı programına benzer TCP ölçümlerini gösterir.

- Verim menüsü

Ortalama verim ve iyi çıktı.

- Gidiş-dönüş süresi menüsü

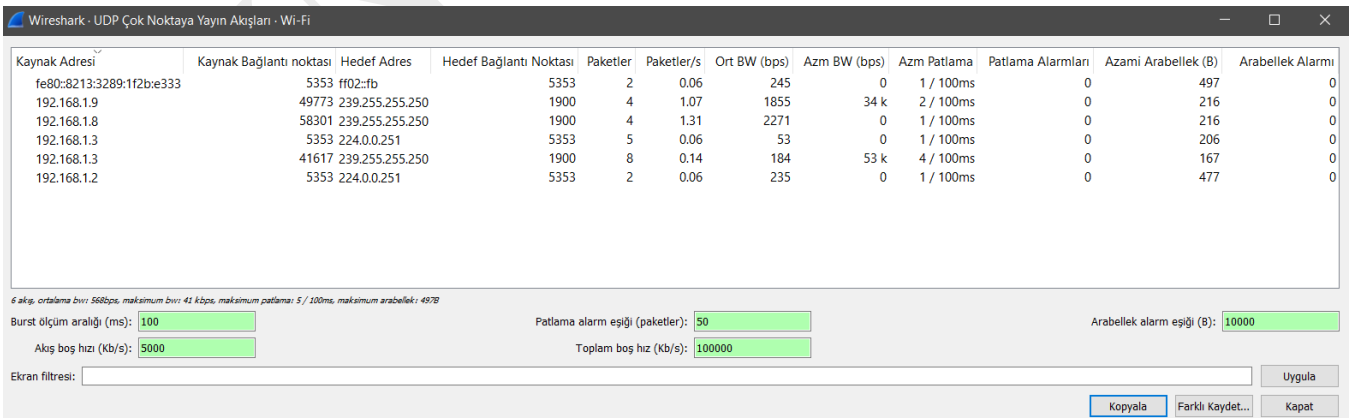
Gidiş-dönüş süresi - zaman veya sıra numarası. RTT, belirli bir segmente karşılık gelen alındı zaman damgasını temel alır.

- Pencere Ölçekleme menüsü

Pencere boyutu ve olağanüstü baytlar.

UDP Çok Noktaya Yayın Akışları: Tüm UDP çok noktaya yayın akışlarının istatistiklerini gösterir. Kaynak adresleri ve portları, hedef adresleri ve portları, paket sayacı ve diğer verileri içerir. Patlama aralığını, alarm limitlerini ve çıkış hızlarını belirleyebilirsiniz. Yeni ayarları uygulamak için <Enter> tuşuna basın. Bu istatistikle şunları yapabilirsiniz:

- Bir video akışı için seri çekim boyutunu ölçün. Bu, sürgülü pencere algoritmasını kullanır.
- Çıkış arabelleği boyutu sınırının, paket düşüşünün oluşmayacağı ölçüsü. Bu, Sızdıran kova algoritmasını kullanır.
- MPEG2 video akışı içindeki paket kaybını tespit edin.



Kaynak Adresi	Kaynak Bağlantı noktası	Hedef Adres	Hedef Bağlantı Noktası	Paketler	Paketler/s	Ort BW (bps)	Azm BW (bps)	Azm Patlama	Patlama Alarmları	Azami Arabellek (B)	Arabellek Alarmı
fe80::8213:3289:1f2b:e333	5353	ff02::fb	5353	2	0.06	245	0	1 / 100ms	0	497	0
192.168.1.9	49773	239.255.255.250	1900	4	1.07	1855	34 k	2 / 100ms	0	216	0
192.168.1.8	58301	239.255.255.250	1900	4	1.31	2271	0	1 / 100ms	0	216	0
192.168.1.3	5353	224.0.0.251	5353	5	0.06	53	0	1 / 100ms	0	206	0
192.168.1.3	41617	239.255.255.250	1900	8	0.14	184	53 k	4 / 100ms	0	167	0
192.168.1.2	5353	224.0.0.251	5353	2	0.06	235	0	1 / 100ms	0	477	0

6 akış, ortalama bittir: 568bps, maksimum bittir: 41 kbps, maksimum patlama: 5 / 100ms, maksimum arabellek: 497B

Burst ölçüm aralığı (ms): 100 Patlama alarm eşiği (paketler): 50 Arabellek alarm eşiği (B): 10000

Akış boş hızı (Kb/s): 5000 Toplam boş hız (Kb/s): 100000

Ekran filtresi: Uygula Kopyala Farklı Kaydet... Kapat

Güvenilir Sunucu Havuzu (RSerPool): Reliable Server Pooling (RSerPool) pencereleri, Reliable Server Pooling'in (RSerPool) farklı protokolleri için istatistikleri gösterir:

- Toplu Sunucu Erişim Protokolü (ASAP)
- Uç Nokta İş Alanı Yedeklilik Protokolü (ENRP)

Ayrıca, RSPLIB tarafından sağlanan uygulama protokolleri için istatistikler de sağlanmaktadır:

- Bileşen Durum Protokolü (CSP)
- CalcApp Protokolü
- Fraktal Jeneratör Protokolü
- Masa tenisi protokolü
- Komut Dosyası Hizmet Protokolü (SSP)

Bu istatistiklerle şunları yapabilirsiniz:

- Mesaj tipi başına gözlemlenen mesaj ve bayt sayısıdır.
- Her mesaj türü için mesajların ve baytların payı.
- Her mesaj türünün ilk ve son oluşumunu görün.
- Her mesaj türünün ilk ve son tekrarı arasındaki aralığa bakın (karşılık gelen türden en az 2 mesaj varsa).
- Her mesaj türü için aralık içindeki mesaj ve bayt hızına bakın (karşılık gelen türden en az 2 mesaj varsa).

F5: F5 Ağlarında TMM, Trafik Yönetimi Mikro Çekirdeği anlamına gelir. BIG-IP sistemindeki tüm yük dengeli trafiği işler. Her ikisi için F5 istatistikleri menü gösterileri paket ve byte sayısı Virtual Server Distribution ve tmm Distribution alt menülerde.

Her Virtual Server Distribution pencere aşağıdaki verilere ilişkin istatistikleri içerir:

- Adlandırılmış her sanal sunucu adı için bir satır.
- Akış kimliği olan ve sanal sunucu adı olmayan trafik için bir satır.
- Akış kimliği olmayan trafik için bir satır.

Her bir giriş ve çıkış için bir satır (toplam tmm'ye eklenmelidir), şunları içerir:

- Sanal sunucu adıyla trafik,
- Akış kimliği olan ve sanal sunucu adı olmayan trafik,
- Akış kimliği olmayan trafik,

IPv4 İstatistikleri: İnternet Protokolü sürüm 4 (IPv4), internet katmanı için bir çekirdek protokoldür. 32 bit adresleri kullanır ve paketlerin bir kaynak ana bilgisayardan diğerine yönlendirilmesine izin verir.

İstatistik/ IPv4 menüde alt menülerin tarafından paket sayacını sağlamaktadır:

- All Addresses menüsü

Verileri IP adresine göre böler.

- Destination and Ports

Verileri IP adresine ve ayrıca TCP, UDP ve diğerleri gibi IP protokol türüne göre böler. Ayrıca port numarasını da gösterir.

- IP Protocol Types

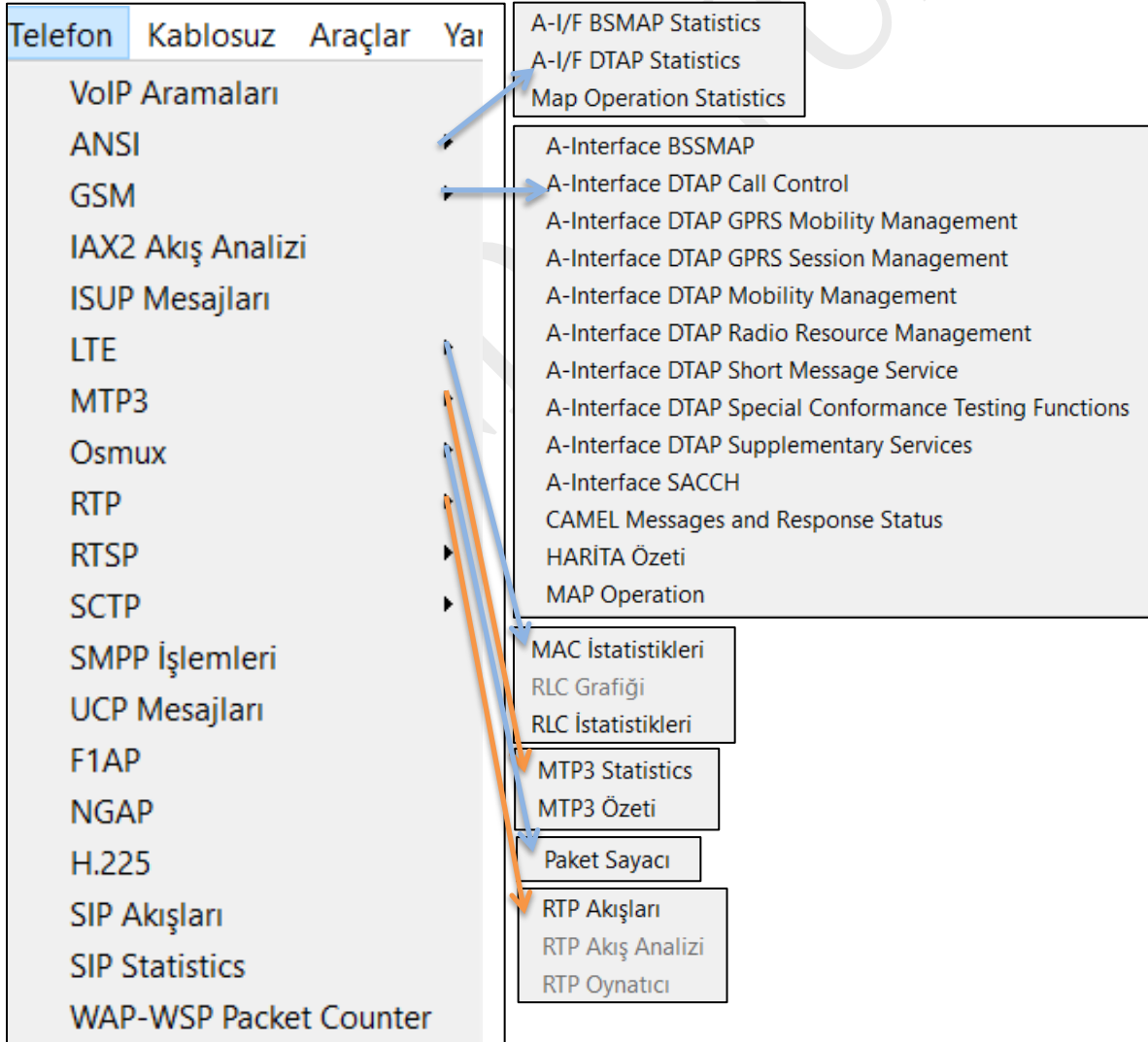
Verileri IP protokol türüne göre böler.

- Source and Destination Addresses

Verileri kaynak ve hedef IP adresine göre böler.

IPv6 İstatistikleri: İnternet Protokolü sürüm 6 (IPv6), internet katmanı için bir çekirdek protokoldür. 128 bit adresleri kullanır ve internet trafiğini yönlendirir.

3.15 TELEFON MENÜSÜ



VoIP Aramaları Penceresi: Yakalanan trafikte algılanan tüm VoIP çağrılarının bir listesini gösterir. Çağrılar sinyalleşmelerine göre bulur ve ilgili RTP akışlarını gösterir. Mevcut VoIP destekli protokoller şunlardır:

- H.323
- IAX2
- ISUP
- MGCP/MEGACO
- Yüklümlamak
- SSKA
- ÜNİSTİM

ANSI: Bu menü, ETSI GSM standartlarına göre mobil iletişim protokolleri için istatistik veri gruplarını gösterir.

- AI/F BSMAP İstatistikleri Penceresi

A-Interface Baz İstasyonu Yönetim Uygulaması Bölümü (BSMAP) İstatistikleri penceresi, mesaj listesini ve yakalanan mesajların sayısını gösterir. Mesajları filtreleme, tarihi kopyalama veya bir dosyaya kaydetme imkânı vardır.

- 9.4.2. AI/F DTAP İstatistikleri Penceresi

A-Interface Direct Transfer Application Part (DTAP) İstatistikleri penceresi, mesaj listesini ve yakalanan mesajların sayısını gösterir. Mesajları filtreleme, tarihi kopyalama veya bir dosyaya kaydetme imkânı vardır.

GSM Pencereleeri: Mobil İletişim için Küresel Sistem (GSM), mobil ağlar için bir standarttır. Bu menü, ETSI GSM standardına göre mobil iletişim protokolleri için bir grup istatistik verisini gösterir.

IAX2 Akış Analizi Penceresi: Bir grafikte birlikte seçilen bir IAX2 çağrısının ileri ve geri akışlarına ilişkin istatistikleri gösterir.

ISUP Mesajları Penceresi: Entegre Hizmet Kullanıcı Parçası (ISUP) protokolü, telefon iletişimleeri için sesli ve sesli olmayan sinyalleşme sağlar. ISUP Mesajları menüsü ilgili istatistikleri gösteren pencereyi açar. Kullanıcı verileri filtreleyebilir, kopyalayabilir veya bir dosyaya kaydedebilir.

LTE:

- LTE MAC Trafik İstatistikleri Penceresi

Yakalanan LTE MAC trafiğinin istatistikleeri. Bu pencere, yakalamada bulunan LTE MAC trafiğini özetleyecektir. Üst bölme, ortak kanallar için istatistikleeri gösterir. Orta bölmedeki her satır, tam olarak bir UE/C-RNTI için istatistiksel vurguları gösterir. Alt bölmede, hali hazırda seçili UE/C-RNTI için ayrı kanala göre ayrılmış trafiği gösterir.

- LTE RLC Grafik Penceresi

LTE RLC Graph menüsü, zaman içinde değişen LTE Radyo Bağlantı Kontrolü protokol sıra numaralarını ve ters yönde alınan alındıları gösteren bir grafiği başlatır.

- LTE RLC Trafik İstatistikleri Penceresi

Yakalanan LTE RLC trafiğinin istatistikleri. Bu pencere, yakalamada bulunan LTE RLC trafiğini özetleyecektir. En üstteki onay kutusu, bu pencerenin MAC PDU'larda bulunan veya bulunmayan RLC PDU'ları içermesine izin verir. Bu, hem sayılan PDU'ları hem de oluşturulan görüntü filtrelerini etkiler. Üstteki liste, her aktif UE'nin özetlerini gösterir. Alt listedeki her satır, seçilen UE içindeki bireysel kanallar için istatistiksel vurguları gösterir. Pencerealt kısmı, seçilen kanal için görüntü filtrelerinin oluşturulmasına ve ayarlanmasına izin verir. Onaylanmış Mod kanalları durumunda, tek bir yön seçilirse, oluşturulan filtrenin verileri o yönde göstereceğini ve PDU'ları ters yönde kontrol edeceğini unutmayın.

MTP3 Pencereleeri: Message Transfer Part level 3 (MTP3) protokolü, Signaling System 7'nin (SS7) bir parçasıdır. Genel Anahtarlama Telefon Ağları bunu, iletişim ortakları arasında SS7 mesajlaşmasının güvenilir, çoğaltılmamış ve sıralı aktarımı için kullanır.

OSmux: Ses proxy'sinin (RTP-AMR) bant genişliği tüketimini ve sinyal trafiğini azaltarak uydu tabanlı GSM geri çekme sistemlerine fayda sağlayan bir multipleks protokolüdür. OSmux menüsü, ilgili istatistik verileriyle birlikte paket sayacı penceresini açar. Kullanıcı verileri filtreleyebilir, kopyalayabilir veya bir dosyaya kaydedebilir.

RTP:

- RTP Akışları Penceresi

RTP akışları penceresi, yakalama dosyasındaki tüm RTP akışlarını gösterir. Akışlar burada seçilebilir ve seçilen akışlarda diğer araçlar başlatılabilir.

- RTP Akış Analizi Penceresi

RTP analiz işlevi, seçilen RTP akışlarını alır ve grafik dâhil olmak üzere bir istatistik listesi oluşturur. Menü Telefon / RTP / RTP Akış Analizi yalnızca seçili paket RTP paketi olduğunda etkinleştirilir. Pencere açıldığında seçilen RTP akışı analize eklenir. Eğer Ctrl menü açılması esnasında basıldığında, (eğer varsa) RTP akışı tersine çok pencere eklenir. Her akış kendi sekmesinde gösterilir. Sekmeler, akışlar eklendikçe numaralandırılır ve araç ipucu, akışın kimliğini gösterir. Sekme kapatıldığında numara tekrar kullanılmaz. Sekmenin rengi, grafik sekmesindeki grafiklerin rengiyle eşleşir.

Paket başına istatistik şunları gösterir:

- Paket numarası
- Sıra numarası
- Delta (ms) son pakete

- Titreşim (ms)
- Eğmek
- Bant genişliği
- İşaretleyici - paket RTP başlığında işaretlenir
- Durum - paketle ilgili bilgiler. Örneğin. codec değişikliği, DTMF numarası, yanlış sıra numarası uyarısı.

Paket listesinin solundaki yan panel, akış istatistiklerini gösterir:

- Maksimal delta ve hangi pakette oluştuğu
- Maksimum titreşim
- Ortalama titreşim
- Maksimum çarpıklık
- Paket sayısı
- Kayıp paketlerin sayısı - sıra numaralarından hesaplanır
- Akış başladığında ve ilk paket numarası
- Akışın süresi
- Saat kayması
- Frekans kayması

○ RTP Oynatıcı Penceresi

RTP Player işlevi, VoIP aramalarını oynatmak için bir araçtır. RTP akışlarını ve dalga biçimlerini gösterir, akışı oynatmaya ve ses olarak veya dosyaya yük olarak dışa aktarmaya izin verir. Menü Telefon / RTP / RTP Oynatıcı yalnızca seçili paket RTP paketi olduğunda etkinleştirilir. Pencere açıldığında seçilen RTP akışı oynatma listesine eklenir. Eğer Ctrl menü açılması esnasında basıldığında, (eğer varsa) RTP akışı tersine çok çalma listesine eklenir.

RTP Player Penceresi üç bölümden oluşur:

1. Dalga formu görünümü
2. Çalma listesi
3. Kontroller

Dalga formu görünümü, RTP akışının görsel sunumunu gösterir. Dalga biçimi ve çalma listesi satırının rengi eşleşiyor. Dalganın yüksekliği hacmi gösterir. Dalga formu, bir akışta gerçekleşirse, Sıra Dışı, Titreşim Düşüşleri, Yanlış Zaman Damgaları ve Eklenen Sessizlik işaretleri için hata işaretleri gösterir.

Oynatma listesi, her akışla ilgili bilgileri gösterir:

- Oynat - Ses yönlendirme
- Kaynak Adresi, Kaynak Bağlantı Noktası, Hedef Adres, Hedef Bağlantı Noktası, SSRC
- Kurulum Çerçevesi

SETUP <sayı>, bilinen bir sinyal paketi olduğunda gösterilir. Sayı, sinyalleme paketinin paket numarasıdır. Not: Sözcük KURULUM, RTP akışı başlatılsa bile gösterilir, örneğin SKINNY tarafından hiçbir SETUP mesajının olmadığı yerde.

İlgili sinyal bulunamadığında RTP <sayı> gösterilir. Sayı, akışın ilk paketinin paket numarasıdır.

Paketler: Akıştaki paketlerin sayısı.

Akışın Zaman Aralığı – Başlangıç: Durdurma (Süre)

SR: Kullanılan codec bileşeninin örnekleme hızı

PR: Akış oynatma için kullanılan kodu çözülmüş oynatma hızı

Yükler: Akış tarafından kullanılan bir veya daha fazla oynatma yükü türü

RTSP Penceresi: Gerçek Zamanlı Akış Protokolü (RTSP) menüsünde, kullanıcı Paket Sayacı penceresini kontrol edebilir. Toplam RTCP Paketlerini gösterir ve RTSP Yanıt Paketleri, RTSP İstek Paketleri ve Diğer RTSP paketlerine bölünmüştür. Kullanıcı verileri filtreleyebilir, kopyalayabilir veya bir dosyaya kaydedebilir.

SCTP Pencereleeri: Akış Kontrol İletim Protokolü (SCTP), taşıma katmanında telekomünikasyonda mesaj aktarımı sağlayan bir bilgisayar ağı protokolüdür. Bazı Kullanıcı Datagram Protokolü (UDP) ve İletim Kontrol Protokolü (TCP) eksikliklerinin üstesinden gelir. SCTP paketleri, ortak başlık ve veri parçalarından oluşur. SCTP Analiz İlişkisi penceresi, iki Uç Nokta arasında yakalanan paketlerin istatistiklerini gösterir. SCTP İlişkilendirmeleri penceresi, bağlantı noktası ve sayaç gibi yakalanan paketler için verileri içeren tabloyu gösterir. Ayrıca Analiz düğmesine basarak SCTP Analiz İlişkilendirme penceresini de arayabilirsiniz.

SMPP İşlemleri: Kısa Mesaj Eşler Arası (SMPP) protokolü, esas olarak Kısa Mesaj Servis Merkezleri (SMSC) arasında Kısa Mesaj Servisi (SMS) Mesajlarının değiş tokuşu için aktarım olarak TCP protokolünü kullanır. Ayırıştırıcı, sabit başlıktaki buluşsal yöntemleri kullanarak yakalanan paketin SMPP olup olmadığını belirler. SMPP İşlemleri penceresi, ilgili istatistiksel verileri görüntüler. Kullanıcı verileri filtreleyebilir, kopyalayabilir veya bir dosyaya kaydedebilir.

UCP Mesajları: Evrensel Bilgisayar Protokolü (UCP), Kısa Mesaj Hizmet Merkezi (SMSC) ile TCP veya X.25 gibi aktarım protokolünü kullanan bir uygulama arasında Kısa Mesajların aktarılmasında rol oynar. UCP Mesajları penceresi, ilgili istatistiksel verileri görüntüler. Kullanıcı verileri filtreleyebilir, kopyalayabilir veya bir dosyaya kaydedebilir.

H.225 Pencere: Paket tabanlı multimedya iletişim sistemleri için çağrı sinyalizasyonu ve medya akışı paketlemesindeki mesajlardan sorumlu olan H.225 telekomünikasyon protokolü. H.225 penceresi, türlere ve nedenlere göre sayılan mesajları gösterir. Kullanıcı verileri filtreleyebilir, kopyalayabilir veya bir dosyaya kaydedebilir.

SIP Akışları: Oturum Başlatma Protokolü (SIP) Akışları penceresi, müşteri kayıtları, mesajlar, çağrılar vb. gibi yakalanan tüm SIP işlemlerinin listesini gösterir. Bu pencere hem tamamlanmış hem de devam eden SIP işlemlerini listeleyecektir. Ayrıca, VoIP Çağrılar penceresiyle aynı özelliklere sahiptir.

SIP İstatistikleri: Yakalanan SIP işlemlerini gösterir. SIP Yanıtları ve SIP İstekleri olarak ikiye ayrılır. Bu pencerede kullanıcı istatistikleri filtreleyebilir, kopyalayabilir veya bir dosyaya kaydedebilir.

WAP-WSP Paket Sayacı: Kablosuz Oturum Protokolü trafiğindeki her Durum Kodu ve PDU Türü için paket sayısını görüntüler. Kullanıcı verileri filtreleyebilir, kopyalayabilir veya bir dosyaya kaydedebilir.

3.16 KABLOSUZ MENÜSÜ

Kablosuz	Araçlar	Yardım
Bluetooth ATT Sunucusu Özellikleri		
Bluetooth Cihazları		
Bluetooth HCI Özeti		
WLAN Trafiği		

Bluetooth ATT Sunucusu Özellikleri: Bluetooth ATT Sunucusu Nitelikleri penceresi, yakalanan Nitelik Protokolü (ATT) paketlerinin bir listesini görüntüler. Kullanıcı, arayüzlere veya cihazlara göre listeyi filtreleyebilir ve ayrıca Remove duplicates onay kutusunu işaretleyerek tekrarları hariç tutabilir.

- Handle cihaza özgü benzersiz bir niteliktir.
- UUID bir özniteliğin türünü tanımlayan bir değerdir.
- UUID Name yakalanan paket için belirtilen addır.

Bluetooth Cihazları: MAC adresi, Organizasyonel Olarak Benzersiz Tanımlayıcı (OUI), Ad ve diğerleri gibi cihazlar hakkında yakalanan bilgilerin listesini görüntüler. Kullanıcılar arayüze göre filtreleyebilir.

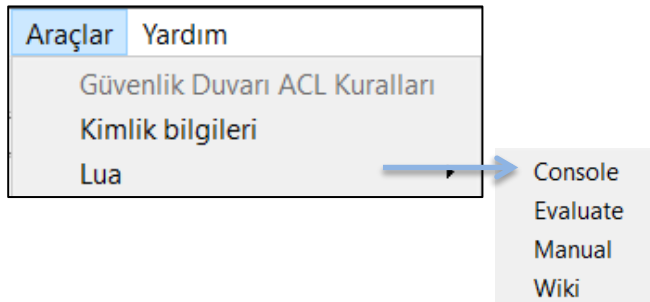
Bluetooth HCI Özeti: Yakalanan Ana Bilgisayar Denetleyici Arayüzü (HCI) katman paketlerinin özetini görüntüler. Bu pencere, kullanıcıların filtreler uygulamasına ve belirli arabirimler veya cihazlarla ilgili bilgileri görüntülemeyi seçmesine olanak tanır.

WLAN Trafiği: Yakalanan WLAN trafiğiyle ilgili istatistikler. Bu, Kablosuz menüsü altında bulunabilir ve yakalamada bulunan kablosuz ağ trafiğini özetler. SSID eşleşirse, araştırma istekleri mevcut bir ağda birleştirilir.

- Listedeki her satır, tam olarak bir kablosuz ağ için istatistiksel değerleri gösterir.

- Ad çözümlemesi, pencerede seçiliyse ve MAC katmanı için etkinse yapılır.
- Yalnızca mevcut ağları göster, listedeki hiçbir ağla eşleşmeyen bir SSID'ye sahip yoklama isteklerini hariç tutacaktır.
- Kopya düğmesi CSV panoya formatına liste değerlerini kopyalar.

3.17 ARAÇLAR MENÜSÜ



Güvenlik Duvarı ACL Kuralları: Cisco IOS, Linux Netfilter (iptables), OpenBSD pf ve Windows Güvenlik Duvarı (netsh aracılığıyla) dâhil olmak üzere birçok farklı güvenlik duvarı ürünü için komut satırı ACL kuralları oluşturmanıza olanak tanır. MAC adresleri, IPv4 adresleri, TCP ve UDP bağlantı noktaları ve IPv4+bağlantı noktası kombinasyonları için kurallar desteklenir.

Kuralların bir dış arayüze uygulanacağı varsayılır.

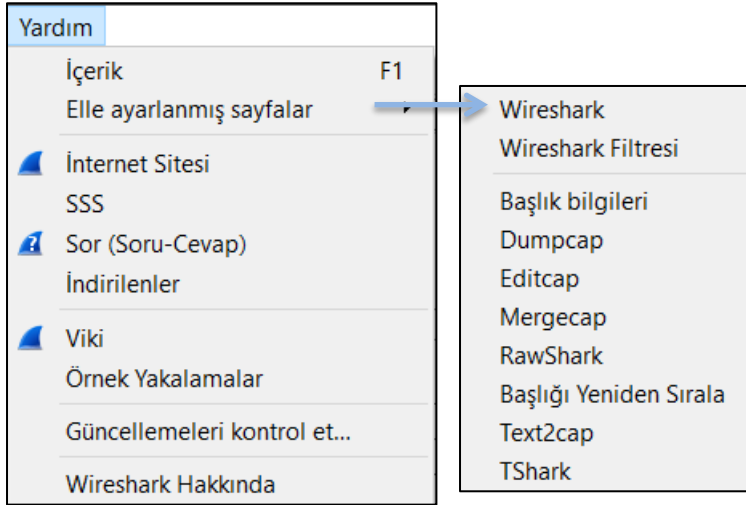
Paket listesinde bir (ve yalnızca bir) çerçeve seçilmediği sürece menü öğesi grileşir.

Kimlik bilgileri: Geçerli yakalama dosyasından kimlik bilgilerini çıkarmanıza olanak tanır. Bazı ayrıştırıcılar (ftp, http, imap, pop, smtp), modüle kullanıcı adları ve şifreler sağlamak için düzenlenmiştir ve gelecekte daha fazlası kullanılacaktır. Pencere iletişim kutusu, kimlik bilgilerinin bulunduğu paket numarasını, bunları sağlayan protokolü, kullanıcı adını ve protokole özel bilgileri sağlar.

Lua: İsteğe bağlı olarak Wireshark' ta yerleşik olarak bulunan Lua yorumlayıcısı ile çalışmanıza izin verir. Wireshark Geliştirici Kılavuzu'ndaki “Wireshark’ ta Lua Desteği” konusuna bakın.

Lua menü yapısı, Wireshark kurulum dizininde console.lua tarafından ayarlanır.

3.18 YARDIM MENÜSÜ



İçerik: Temel bir yardım sistemini getirir.

Elle Ayarlanmış Sayfalar: Yerel olarak kurulmuş html kılavuz sayfalarından birini gösteren bir Web tarayıcısını başlatır.

İnternet Sitesi: <https://www.wireshark.org/> adresinden web sayfasını gösteren bir Web tarayıcısını başlatır.

SSS: Çeşitli SSS'leri gösteren bir Web tarayıcısını başlatır.

İndirilenler: İndirmeleri gösteren bir Web tarayıcısını başlatır:
<https://www.wireshark.org/download.html>

Viki: Ön sayfayı gösteren bir Web tarayıcısını başlatır:
<https://gitlab.com/wireshark/wireshark/wikis/>

Örnek Yakalamalar: Örnek yakalamaları gösteren bir Web tarayıcısını başlatır:
<https://gitlab.com/wireshark/wireshark/wikis/SampleCaptures>

Wireshark Hakkında: Nasıl oluşturulduğu, yüklenen eklentiler, kullanılan klasörler gibi Wireshark hakkında çeşitli ayrıntılı bilgi öğeleri sağlayan bir bilgi penceresi açar.

Not: Wireshark sürümünüzde bir Web tarayıcısının açılması desteklenmiyor olabilir. Bu durumda ilgili menü öğeleri gizlenecektir.

Makinenizde bir Web tarayıcısının çağırılması başarısız olursa, hiçbir şey olmuyorsa veya tarayıcı başlatılıyor ancak hiçbir sayfa görüntülenmiyorsa, tercihler iletişim kutusundaki web tarayıcısı ayarına bakın.

FUNDA YÜKSEL