Pacotes do wireshark para você fazer download e verificar o handshake e outros tipos de ataques e problemas.

Use os filtros estabelecidos nos sites de referências para entender como achar as portas, pacotes e protocolos.

https://wiki.wireshark.org/TCP_3_way_handshaking

Aqui está o arquivo para análise do 3_way_handshaking

https://wiki.wireshark.org/TCP_3_way_handshaking?action=AttachFile&do=view&target=3-way+handshake.pcap

tfp_capture.pcapng (libpcap) Tinkerforge protocol captures over TCP/IP and USB.

NTLM.pcap (libpcap) Illustrate NTLM authentication process, based on WSS 3.0

Obsolete_Packets.cap (libpcap) Contains various obscure/no longer in common use protocols, including Banyan VINES, AppleTalk and DECnet.

Apple_IP-over-IEEE_1394_Packet.pcap (libpcap) An ICMP packet encapsulated in Apple's IP-over-1394 (ap1394) protocol

SkypeIRC.cap (libpcap) Some Skype, IRC and DNS traffic.

ipp.pcap (libpcap) CUPS printing via IPP (test page)

IrDA_Traffic.ntar (pcap-ng) Various IrDA packets, use Wireshark 1.3.0 (SVN revision 28866 or higher) to view

9p.cap (libpcap) Plan 9 9P protocol, various message types.

EmergeSync.cap (libpcap) rsync packets, containing the result of an "emerge sync" operation on a Gentoo system

afs.cap.gz (libpcap) Andrew File System, based on RX protocol. Various operations.

ancp.pcap.gz (libpcap) Access Node Control Protocol (ANCP).

ascend.trace.gz (Ascend WAN router) Shows how Wireshark parses special Ascend data

atm_capture1.cap (libpcap) A trace of ATM Classical IP packets.

bacnet-arcnet.cap (libpcap) Some BACnet packets encapsulated in ARCnet framing bfd-raw-auth-simple.pcap (libpcap) BFD packets using simple password authentication.

bfd-raw-auth-md5.pcap (libpcap) BFD packets using md5 authentication.

bfd-raw-auth-sha1.pcap (libpcap) BFD packets using SHA1 authentication.

BT_USB_LinCooked_Eth_80211_RT.ntar.gz (pcap-ng) A selection of Bluetooth, Linux mmapped USB, Linux Cooked, Ethernet, IEEE 802.11, and IEEE 802.11 RadioTap packets in a pcap-ng file, to showcase the power of the file format, and Wireshark's support for it. Currently, Wireshark doesn't support files with multiple Section Header Blocks, which this file has, so it cannot read it. In addition, the first packet in the file, a Bluetooth packet, is corrupt - it claims to be a packet with a Bluetooth pseudo-header, but it contains only 3 bytes of data, which is too small for a Bluetooth pseudo-header.

bootparams.cap.gz (libpcap) A couple of rpc.bootparamsd 'getfile' and 'whoami' requests.

cmp_IR_sequence_OpenSSL-Cryptlib.pcap (libpcap) Certificate Management Protocol (CMP) version 2 encapsulated in HTTP. Full "Initialization Request".

cmp_IR_sequence_ OpenSSL-EJBCA.pcap (libpcap) Certificate Management Protocol (CMP) version 2 encapsulated in HTTP. Full "Initialization Request". Authentication with CRMF regToken.

cmp-trace.pcap.gz (libpcap) Certificate Management Protocol (CMP) certificate requests.

cmp-in-http-with-errors-in-cmp-protocol.pcap.gz (libpcap) Certificate Management Protocol (CMP) version 2 encapsulated in HTTP. Full "Initialization Request" and rejected "Key Update Request". There are some errors in the CMP packages.

cmp_in_http_with_pkixcmp-poll_content_type.pcap.gz (libpcap) Certificate Management Protocol (CMP) version 2 encapsulated in HTTP. The CMP messages are of the deprecated but used content-type "pkixcmp-poll", so they are using the TCP transport style. In two of the four CMP messages, the content type is not explicitly set, thus they cannot be dissected correctly.

cigi2.pcap.gz (libpcap) Common Image Generator Interface (CIGI) version 2 packets.

cigi3.pcap.gz (libpcap) Common Image Generator Interface (CIGI) version 3 packets.

ciscowl.pcap.gz (libpcap) Cisco Wireless LAN Context Control Protocol (WLCCP) version 0x0

ciscowl_version_0xc1.pcap.gz (libpcap) Cisco Wireless LAN Context Control Protocol (WLCCP) version 0xc1. Includes following base message types: SCM Advertisements, EAP Auth., Path Init, Registration

configuration_test_protocol_aka_loop.pcap (libpcap) Example of an Ethernet loopback with a 'third party assist'

cops-pr.cap.gz (libpcap) A sample of COPS traffic.

couchbase_subdoc_multi.pcap (libpcap) A sample Couchbase binary protocol file including sub-document multipath request/responses.

couchbase-create-bucket.pcapng (libpcap) A sample Couchbase binary protocol file that includes a create_bucket command.

couchbase-lww.pcap (libpcap) A sample Couchbase binary protocol file including set_with_meta, del_with_meta and get_meta commands with last write wins support.

couchbase-xattr.pcapng (libpcap) A sample capture of the XATTR features in the Couchbase binary protocol.

dct2000_test.out (dct2000) A sample DCT2000 file with examples of most supported link types

dhcp.pcap (libpcap) A sample of DHCP traffic.

dhcp-and-dyndns.pcap.gz (libpcap) A sample session of a host doing dhcp first and then dyndns.

dhcp-auth.pcap.gz (libpcap) A sample packet with dhcp authentication information.

PRIV_bootp-both_overload.pcap (libpcap) A DHCP packet with sname and file field overloaded.

PRIV_bootp-both_overload_empty-no_end.pcap (libpcap) A DHCP packet with overloaded field and all end options missing.

dccp_trace.pcap.gz (libpcap) A trace of DCCP packet types.

dns.cap (libpcap) Various DNS lookups.

dualhome.iptrace (AIX iptrace) Shows Ethernet and Token Ring packets captured in the same file.

dvmrp-conv.cap Shows Distance Vector Multicast Routing Protocol packets.

eapol-mka.pcap (libpcap) EAPoL-MKA (MKA, IEEE 802.1X) traffic.

epmd.pcap Two Erlang Port Mapper Daemon (EPMD) messages.

Ethernet_Pause_Frame.cap Ethernet Pause Frame packets.

exec-sample.pcap The exec (rexec) protocol

genbroad.snoop (Solaris snoop) Netware, Appletalk, and other broadcasts on an ethernet network.

Mixed1.cap (MS NetMon) Some Various, Mixed Packets.

gryphon.cap (libpcap) A trace of Gryphon packets. This is useful for testing the Gryphon plug-in.

hart_ip.pcap (libpcap) Some HART-IP packets, including both an UDP and TCP session.

hsrp.pcap (libpcap) Some Cisco HSRP packets, including some with Opcode 3 (Advertise) .

hsrp-and-ospf-in-LAN (libpcap) HSRP state changes and OSPF LSAs sent during link up/down/up.

ipv4_cipso_option.pcap (libpcap) A few IP packets with CIPSO option.

imap.cap.gz (libpcap) A short IMAP session using Mutt against an MSX server.

RawPacketIPv6Tunnel-UK6x.cap (libpcap) - Some IPv6 packets captured from the 'sit1' interface on Linux. The IPv6 packets are carried over the UK's UK6x network, but what makes this special, is the fact that it has a Link-Layer type of "Raw packet data" - which is something that you don't see everyday.

iseries.cap (IBM iSeries communications trace) FTP and Telnet traffic between two AS/400 LPARS.

FTPv6-1.cap (Microsoft Network Monitor) FTP packets (IPv6)

FTPv6-2.cap (Microsoft Network Monitor) Some more FTP packets (IPv6)

gearman.cap Gearman Protocol packets

isl-2-dot1q.cap (libpcap) A trace including both ISL and 802.1q-tagged Ethernet frames. Frames 1 through 381 represent traffic encapsulated using Cisco's ISL, frames 382-745 show traffic sent by the same switch after it had been reconfigured to support 802.1Q trunking.

kafka-testcases-v4.tar.gz (libpcap) Apache Kafka dissector testcases (generated with this scripts).

lacp1.pcap.gz (libpcap) Link Aggregation Control Protocol (LACP, IEEE 802.3ad) traffic.

linx-setup-pingpong-shutdown.pcap (libpcap) Successive setup of LINX on two hosts, exchange of packets and shutdown.

llrp.cap EPCglobal Low-Level Reader Protocol (LLRP)

llt-sample.pcap Veritas Low Latency Transport (LLT) frames

macsec_cisco_trunk.pcap (libpcap) MACsec/802.1AE session, manual keys, 3750X switch-to-switch (Trustsec) forced across a half-duplex 10M hub connection, destination mac addresses can be seen for Cisco VTP, RSTP (RPVST+), CDP, EIGRP etc.

mapi.cap.gz (libpcap) MAPI session w/ Outlook and MSX server, not currently decoded by Wireshark.

messenger.pcap (libpcap) a few messenger example packets.

metamako_trailer.pcap (libpcap) the Metamako timestamp trailer format.

mms.pcap.gz (libpcap) Manufacturing Message Specification traffic.

SITA-Protocols.cap (libpcap) Some SITA WAN (Societe Internationale de Telecommunications Aeronautiques sample packets (contains X.25, International Passenger Airline Reservation System, Unisys Transmittal System and Frame Relay packets)

msnms.pcap (libpcap) MSN Messenger packets.

MSN_CAP.xlsx (xlsx) MSN Messenger packets in xlsx format.

monotone-netsync.cap.gz (libpcap) Some fragments (the full trace is > 100MB gzipped) of a checkout of the monotone sources.

mpeg2_mp2t_with_cc_drop01.pcap (libpcap) MPEG2 (RFC 2250) Transport Stream example with a dropped CC packet (anonymized with tcpurify).

mpls-basic.cap (libpcap) A basic sniff of MPLS-encapsulated IP packets over Ethernet.

mpls-exp.cap (libpcap) IP packets with EXP bits set.

mpls-te.cap (libpcap) MPLS Traffic Engineering sniffs. Includes RSVP messages with MPLS/TE extensions and OSPF link updates with MPLS LSAs.

mpls-twolevel.cap (libpcap) An IP packet with two-level tagging.

netbench_1.cap (libpcap) A capture of a reasonable amount of NetBench traffic. It is useful to see some of the traffic a NetBench run generates.

NMap Captures.zip (libpcap) Some captures of various NMap port scan techniques.

OptoMMP.pcap A capture of some OptoMMP read/write quadlet/block request/response packets. OptoMMP documentation.

pana.cap (libpcap) PANA authentication session (pre-draft-15a so Wireshark 0.99.5 or before is required to view it correctly).

pana-draft18.cap (libpcap) PANA authentication session (draft-18 so Wireshark 0.99.7 or later is required to view it correctly).

pana-rfc5191.cap (libpcap) PANA authentication and re-authentication sequences.

pim-reg.cap (libpcap) Protocol Independent Multicast, with IPv6 tunnelled within IPv6

ptpv2.pcap (libpcap) various Precision Time Protocol (IEEE 1588) version 2 packets.

Public_nic (libpcap) A bunch of SSDP (Universal Plug and Play protocol) announcements.

rpl_sample.cap.gz (libpcap) A RIPL sample capture.

rtp_example.raw.gz (libpcap) A VoIP sample capture of a H323 call (including H225, H245, RTP and RTCP).

rtps_cooked.pcapng (libpcap) Manually generated RTPS traffic covering a range of submessages and parameters.

rsvp-PATH-RESV.pcap (libpcap) A sample RSVS capture with PATH and RESV messages.

sbus.pcap (libpcap) An EtherSBus (sbus) sample capture showing some traffic between the programming tool (PG5) and a PCD (Process Control Device, a PLC; Programmable Logic Controller).

Ether-S-IO_traffic_01.pcap.gz (libpcap) An EtherSIO (esio) sample capture showing some traffic between a PLC from Saia-Burgess Controls AG and some remote I/O stations (devices called PCD3.T665).

simulcrypt.pcap (libpcap) A SIMULCRYPT sample capture, SIMULCRYPT over TCP) on ports 8600, 8601, and 8602.

TeamSpeak2.pcap (libpcap) A TeamSpeak2 capture

tipc-publication-payload-withdrawal.pcap (libpcap) TIPC port name publication, payload messages and port name withdrawal.

tipc-bundler-messages.pcap (libpcap) TIPCv2 Bundler Messages

tipc_v2_fragmenter_messages.pcap.gz (libpcap) TIPCv2 Fragmenter Messages

TIPC-over-TCP_disc-publ-inventory_sim-withd.pcap.gz (libpcap) TIPCv2 over TCP (port 666) traffic generated by the inventory simulation of the TIPC demo package.

TIPC-over-TCP_MTU-discovery.pcap.gz (libpcap) TIPCv2 over TCP (port 666) - Link State messages with filler bytes for MTU discovery.

toshiba.general.gz (Toshiba) Just some general usage of a Toshiba ISDN router. There are three link types in this trace: PPP, Ethernet, and LAPD.

uma_ho_req_bug.cap (libpcap) A "UMA URR HANDOVER REQUIRED" packet.

unistim_phone_startup.pcap (libpcap) Shows a phone booting up, requesting ip address and establishing connection with cs2k server.

unistim-call.pcap (libpcap) Shows one phone calling another via cs2k server over unistim

v6.pcap (libpcap) Shows IPv6 (6-Bone) and ICMPv6 packets.

v6-http.cap (libpcap) Shows IPv6 (SixXS) HTTP.

vlan.cap.gz (libpcap) Lots of different protocols, all running over 802.1Q virtual lans.

vms_tcptrace.txt (VMS TCPtrace) Sample output from VMS TCPtrace. Mostly NFS packets.

vms_tcptrace-full.txt (VMS TCPtrace) Sample output from VMS TCPtrace/full. Mostly NFS packets.

vnc-sample.pcap Virtual Networking Computing (VNC) session trace

vxi-11.pcap.gz (libpcap) Scan for instruments attached to an Agilent E5810A VXI-11-to-GPIB adapter.

WINS-Replication-01.cap.gz (libpcap) WINS replication trace.

WINS-Replication-02.cap.gz (libpcap) WINS replication trace.

WINS-Replication-03.cap.gz (libpcap) WINS replication trace.

wpsdata.cap (libpcap) WPS expanded EAP trace.

openwire_sample.tar.gz (libpcap) ActiveMQ OpenWire trace.

drda_db2_sample.tgz (libpcap) DRDA trace from DB2.

starteam_sample.tgz (libpcap) StarTeam trace.

rtmp_sample.tgz (libpcap) RTMP (Real Time Messaging Protocol) trace.

rtmpt.pcap.bz2 (libpcap) RTMPT trace with macromedia-fsc TCP-stuff.

sample-imf.pcap.gz (libpcap) SMTP and IMF capture. Also shows some MIME_multipart.

smtp.pcap (libpcap) SMTP simple example.

captura.NNTP.cap (libpcap) NNTP News simple example.

sample-TNEF.pcap.gz (libpcap) TNEF trace containing two attachments as well as message properties. Also shows some SMTP, IMF and MIME_multipart trace.

wol.pcap (libpcap) WakeOnLAN sample packets generated from both ether-wake and a Windows-based utility.

zigbee-join-authenticate.pcap.gz (libpcap) Two devices join a ZigBee network and authenticate with the trust center. Network is encrypted using network keys and trust center link keys.

IGMP dataset.pcap (igmp) igmp version 2 dataset

yami.pcap (yami) sample packets captured when playing with YAMI4 library

DHCPv6.pcap (dhcpv6) sample dhcpv6 client server transaction solicit(fresh lease)/advertise/request/reply/release/reply.

dhcpv6.pcap (dhcpv6) sample dhcpv6 client server transaction solicit(requesting-old-lease)/advertise/request/reply/release/reply.

Referencias:

https://wiki.wireshark.org/SampleCaptures

http://www.lovemytool.com/blog/2010/05/wireshark-and-tshark-decrypt-sample-capture-file-by-joke-snelders.html

http://www.thegeekstuff.com/2012/07/wireshark-filter/