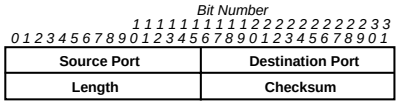
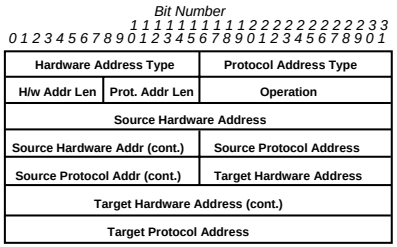
UDP Header



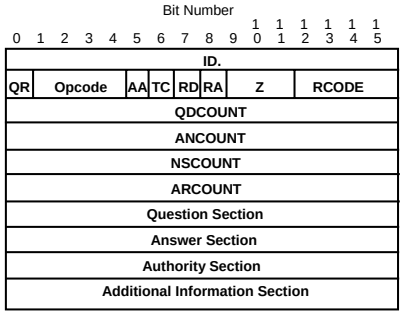

```
UDP Header information
-------------------------------------
Common UDP Well-Known Server Ports
    7 echo              138 netbios-dgm
   19 chargen           161 snmp
   37 time              162 snmp-trap
   53 domain            500 isakmp
   67 bootps (DHCP)     514 syslog
   68 bootpc (DHCP)     520 rip
   69 tftp            33434 traceroute
  137 netbios-ns
Length (Number of bytes in entire datagram
  including header; minimum value = 8)
Checksum (Covers pseudo-header and entire
  UDP datagram)
```

ARP




```
ARP Parameters (for Ethernet and IPv4)
-------------------------------------
Hardware Address Type
  1 Ethernet
  6 IEEE 802 LAN
Protocol Address Type
  2048 IPv4 (0x0800)
Hardware Address Length
  6 for Ethernet/IEEE 802
Protocol Address Length
  4 for IPv4
Operation
  1 Request
  2 Reply
```

DNS




```
DNS Parameters
--------------------------------------
Query/Response
  0 Query
  1 Response
Opcode
  0 Standard query (QUERY)
  1 Inverse query (IQUERY)
  2 Server status request (STATUS)
AA (1 = Authoritative Answer)
TC (1 = TrunCation)
RD (1 = Recursion Desired)
RA (1 = Recursion Available)
Z (Reserved; set to 0)
Response code
  0 No error
  1 Format error
  2 Server failure
  3 Non-existant domain (NXDOMAIN)
  4 Query type not implemented
  5 Query refused
QDCOUNT (No. of entries in Question section)
ANCOUNT (No. of resource records in Answer section)
NSCOUNT (No. of name server resource records in
  Authority section)
ARCOUNT (No. of resource records in Additional
  Information section.
```

All TCP/IP parameters can be found at *http://www.iana.org/numbers.htm*.

Acronyms

AH	Authentication Header (RFC 2402)
ARP	Address Resolution Protocol (RFC 826)
BGP	Border Gateway Protocol (RFC 1771)
CWR	Congestion Window Reduced (RFC 2481)
DF	Don't Fragment bit (IP)
DHCP	Dynamic Host Configuration Protocol (RFC 2131)
DNS	Domain Name System (RFC 1035)
ECN	Explicit Congestion Notification (RFC 3168)
EIGRP	Extended IGRP (Cisco)
ESP	Encapsulating Security Payload (RFC 2406)
FTP	File Transfer Protocol (RFC 959)
GRE	Generic Routing Encapsulation (RFC 2784)
HTTP	Hypertext Transfer Protocol (RFC 1945)
ICMP	Internet Control Message Protocol (RFC 792)
IGMP	Internet Group Management Protocol (RFC 2236)
IGRP	Interior Gateway Routing Protocol (Cisco)
IMAP	Internet Message Access Protocol (RFC 2060)
IP	Internet Protocol (RFC 791)
ISAKMP	Internet Security Association & Key Management Protocol (RFC 2408)
L2TP	Layer 2 Tunneling Protocol (RFC 2661)
NNTP	Network News Transfer Protocol (RFC 977)
OSPF	Open Shortest Path First (RFC 1583)
POP3	Post Office Protocol v3 (RFC 1460)
RFC	Request for Comments
RIP	Routing Information Protocol (RFC 2453)
LDAP	Lightweight Directory Access Protocol (RFC 2251)
SKIP	Simple Key management for Internet Protocols
SMTP	Simple Mail Transfer Protocol (RFC 821)
SNMP	Simple Network Management Protocol (RFC 1157)
SSH	Secure Shell
SSL	Secure Sockets Layer (Netscape)
TCP	Transmission Control Protocol (RFC 793)
TFTP	Trivial File Transfer Protocol (RFC 1350)
TOS	Type of Service field (IP)
UDP	User Datagram Protocol (RFC 768)

All RFCs can be found at *http://www.rfc-editor.org*.

Champlain College
Gary C. Kessler
+1 802-865-6460
gary.kessler@champlain.edu
http://digitalforensics.champlain.edu

TCP/IP and tcpdump Pocket Reference Guide

tcpdump Usage

```
tcpdump [-aenStvx] [-F file]
[-i int] [-r file] [-s snaplen]
[-w file] ['filter_expression']

-e  Display data link header.
-F  Filter expression in file.
-i  Listen on int interface.
-n  Don't resolve IP addresses.
-r  Read packets from file.
-s  Get snaplen bytes from each
    packet.
-S  Use absolute TCP sequence
    numbers.
-t  Don't print timestamp.
-v  Verbose mode.
-w  Write packets to file.
-x  Display in hex.
-X  Display in hex and ASCII.
```

© 2002-2006, Gary Kessler

ICMP

Bit Number

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type	Code	Checksum
Other message-specific information...		

```
Type Name/Codes (Code=0 unless otherwise specified)
---- ------------------------------------------------
  0  Echo Reply
  3  Destination Unreachable
       0 Net Unreachable
       1 Host Unreachable
       2 Protocol Unreachable
       3 Port Unreachable
       4 Fragmentation Needed & DF Set
       5 Source Route Failed
       6 Destination Network Unknown
       7 Destination Host Unknown
       8 Source Host Isolated
       9 Network Administratively Prohibited
      10 Host Administratively Prohibited
      11 Network Unreachable for TOS
      12 Host Unreachable for TOS
      13 Communication Administratively Prohibited
  4  Source Quench
  5  Redirect
       0 Redirect Datagram for the Network
       1 Redirect Datagram for the Host
       2 Redirect Datagram for the TOS & Network
       3 Redirect Datagram for the TOS & Host
  8  Echo
  9  Router Advertisement
 10  Router Selection
 11  Time Exceeded
       0 Time to Live exceeded in Transit
       1 Fragment Reassembly Time Exceeded
 12  Parameter Problem
       0 Pointer indicates the error
       1 Missing a Required Option
       2 Bad Length
 13  Timestamp
 14  Timestamp Reply
 15  Information Request
 16  Information Reply
 17  Address Mask Request
 18  Address Mask Reply
 30  Traceroute
```

PING (Echo/Echo Reply)

Bit Number

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type (8 or 0)	Code (0)	Checksum
Identifier		Sequence Number
Data...		

IP Header

Bit Number

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol		Header Checksum
Source Address			
Destination Address			
Options (optional)			

```
IP Header Contents
----------------------------------------------------------
Version
  4 IP version 4
Internet Header Length
  Number of 32-bit words in IP header; minimum
  value = 5 (20 bytes) & maximum value = 15 (60 bytes)
Type of Service (PreDTRCx) --> Differentiated Services
  Precedence (000-111)           000
  D (1 = minimize delay)         0
  T (1 = maximize throughout)    0
  R (1 = maximize reliability)   0
  C (1 = minimize cost)          1 = ECN capable
  x (reserved and set to 0)      1 = congestion experienced
Total Length
  Number of bytes in packet; maximum length = 65,535
Flags (xDM)
  x (reserved and set to 0)
  D (1 = Don't Fragment)
  M (1 = More Fragments)
Fragment Offset
  Position of this fragment in the original datagram,
  in units of 8 bytes
Protocol
   1 ICMP           17 UDP          57 SKIP
   2 IGMP           47 GRE          88 EIGRP
   6 TCP            50 ESP          89 OSPF
   9 IGRP           51 AH          115 L2TP
Header Checksum
  Covers IP header only
Addressing
       NET_ID            RFC 1918 PRIVATE ADDRESSES
    0-127 Class A        10.0.0.0-10.255.255.255
  128-191 Class B        172.16.0.0-172.31.255.255
  192-223 Class C        192.168.0.0-192.168.255.255
  224-239 Class D (multicast)
  240-255 Class E (experimental)
      HOST_ID
    0 Network value; broadcast (old)
  255 Broadcast
Options (0-40 bytes; padded to 4-byte boundary)
  0 End of Options list      68 Timestamp
  1 No operation (pad)      131 Loose source route
  7 Record route            137 Strict source route
```

TCP Header

Bit Number

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Source Port			Destination Port
Sequence Number			
Acknowledgment Number			
Offset	Reserved	Flags	Window
Checksum			Urgent Pointer
Options (optional)			

```
TCP Header Contents
-----------------------------------------------
Common TCP Well-Known Server Ports
   7 echo           110 pop3
  19 chargen        111 sunrpc
  20 ftp-data       119 nntp
  21 ftp-control    139 netbios-ssn
  22 ssh            143 imap
  23 telnet         179 bgp
  25 smtp           389 ldap
  53 domain         443 https (ssl)
  79 finger         445 microsoft-ds
  80 http          1080 socks
Offset
  Number of 32-bit words in TCP header;
  minimum value = 5
Reserved
  4 bits; set to 0
  ECN bits (used when ECN employed; else 00)
    CWR (1 = sender has cut congestion
             window in half)
    ECN-Echo (1 = receiver cuts congestion
              window in half)
Flags (UAPRSF)
  U (1 = Urgent pointer valid)
  A (1 = Acknowledgement field value valid)
  P (1 = Push data)
  R (1 = Reset connection)
  S (1 = Synchronize sequence numbers)
  F (1 = no more data; Finish connection)
Checksum
  Covers pseudoheader and entire TCP segment
Urgent Pointer
  Points to the sequence number of the byte
  following urgent data.
Options
  0 End of Options list    3 Window scale
  1 No operation (pad)     4 Selective ACK ok
  2 Maximum segment size   8 Timestamp
```