CYBRARY

Section 1 - Sniffer Glossary

1. **ACK flag -** The acknowledgement flag is part of the TCP three-way handshake, and indicates a packet was successfully received by the intended host. It is used in sniffing techniques to determine if a host is protected by a firewall or another filtering system. For example, if a stateful firewall is protecting the network, it will ignore an ACK from an attacker. If the network is unprotected, the RST response will be sent from a targeted host. If the sniffer trace shows nothing, it is an indication that a firewall is configured and working.
   SOURCE: KeyCDN, 2018.
2. **Address Resolution Protocol (ARP) -** Used to resolve an IP address to a machine address on a local network. In protocol analysis, the process can be viewed as an ARP broadcast used to resolve the IP address to the machine address, which is also information used in the ARP cache of the machine.
   SOURCE: Gregg & Santos 2019.
3. **Advanced Message Queueing Protocol (AMQP) -** An open standard for passing business messages between applications or organizations; it connects systems and provides business processes with the data needed to forward instructions; can handling high-volume data streams with low-latency.
   SOURCE: Lane, 2018.
4. **Authentication Header (AH) -** A connectionless oriented IPsec protocol that provides authentication, integrity, and nonrepudiation, by using hash functions and shared secret keys, added to the beginning of an IP datagram.
   SOURCE: Chapple, Stewart, & Gibson, 2018.
5. **AVTP Audio Format -** In Wireshark, this indicates packets that are formatted for transmitting audio. All packets in the stream are the same size and each packet contains a timestamp that corresponds to the first sample in the packet. The payload headers are specific: 10 bits per channel frame, 2 bits for synchronized markers, and 4 bits reserved for future use. A header contains information needed for an end station to determine the payload format.
   SOURCE: Jones & Butterworth, 2015.
6. **ASCII -** Abbreviations for American Standard Code for Information Interchange. Originally developed for teletype, it is the raw, unformatted, plaintext, used by computers to understand characters, symbols, and numbers coded in lookup tables, usually in hexadecimal numbers and letters.
   SOURCES**:** CSRS, 2019.
7. **Bad Checksum -** A value computed on data to detect error or manipulation of the data. It is used to verify or to indicate if the data integrity is compromised. A bad checksum indicates the code (or data) has been modified.
   SOURCE: NIST SP 800-128, 2011.

8. **Bridge-ID (BID) -** In creating and using spanning tree protocol (STP), each VLAN will provide this information about the local switch (where commands are executed). Each switch has a Bridge ID. Each BID has a priority value and a MAC address.
   SOURCE: Cisco, 2009.
9. **Broadcast -** Transmission to all devices in a network without any acknowledgement by the receivers. The sender does not need to know the IP address of the devices to which the broadcast is sent.
   SOURCE: NIST SP 800-82, 2015.
10. **Capture/Capturing -** Term used to describe sniffing a live packet from a physical network interface. The Wireshark capture library (libpcap/WinPcap) can capture data on both physical and virtual network interfaces, of different types of platforms (e.g., Linux, Windows).
    SOURCE: Wireshark, 2019.
11. **Capture File/Open Files -** Files containing live captured data packets. The capture files can be edited or configured to dissect hundreds of network protocols. Wireshark filters can parse traffic captures and save the output in various formats. In tcpdump, expressions are used to match packets against a selected filter, which can be used when starting or replacing a capture file. (See Open Capture File).
    SOURCE: Carnegie Mellon. (2009).
12. **Capture Filter -** A syntax tool used to specify the type of raw data packets to be captured on the physical or virtual interface. The filter is set before the capture and can not be altered during the process. For example, “Capture only DNS (port 53) traffic,” or “Capture traffic from IP 192.168.0.0.”
    SOURCE: Wireshark, 2019.
13. **Certified Ethical Hacker (CEH) -** A skilled professional who is trained in legally uncovering weaknesses and vulnerabilities in a target system for the benefit of helping an organization improve security by mitigating discovered vulnerabilities. The goal of the CEH is to undertake preventive, corrective, and protective countermeasures before an actual compromise occurs in a system. The CEH certification is established by the EC-Council.
    SOURCE: EC-Council, 2019.
14. **Checksum -** A created value generated from an encryption algorithm between data and an object. The value is either stored or transmitted with the object and is used to detect modifications to the data.
    SOURCE: CNSSI No. 2009, 2015.
15. **Cleartext -** Known also as plaintext. In sniffing, cleartext is any data that is unencrypted and can be plainly viewed or read in a data capture. The plaintext may be unencrypted code input that can be seen or packets in transit that can be sniffed.
    SOURCE: NIST SP 800-38F, 2012.
16. **Cookie -** Small file that stores information for a web site in a computer’s web browser. Cookies may be HTTP cookies, persistent cookies, or session cookies. A message is sent

CYBRARY

back to the web server each time the browser visits the associated website and is used to maintaining the state that is otherwise a stateless connection.
SOURCE: Gregg & Santos, 2019.

17. **Decnet -** A protocol suite and architecture that is used to connect devices and machines on ethernet segments and networks. It was created by the Digital Equipment Corporation and is a proprietary protocol. In tcpdump, the associated decent include: decnet host, decnet src, decnet dst.
SOURCE: The Free Dictionary, 2003.
18. **Defragmentation Error -** Found in the Windows registry under the local HKEY, this is a code used to indicate specific error types. For example, “10 = invalid drive, or 106 = could not access drive,” or other results. The defragmentation process itself is used to reverse fragmentation that occurs in a hard drive’s memory module.
SOURCE: Fisher, 2019.
19. **Destination Host -** As it pertains to protocol analysis, this term refers to Transport Layer 4 and destination port numbers that identify a service listening on a destination host (target host) and a source port (the communication path is between the source host and the destination host, which sends a reply). A packet capture will display protocols with ports (e.g. TCP and UDP), to show the source IP and port, and destination IP and port, which defines the actual session.
SOURCE: NIST SP 800-41, 2009.
20. **Destination IP Address -** In reading a sniffer trace, the destination IP address will provide you with information on the IP address, the port, and the connection state. For example, a source address 192.168.1.100 from source port 1030 showing packets going to a destination address of 192.0.2.71 on destination port 80, will indicate if the connection state is initiated or established. Most protocols are connectionless and do not have a formal process for initializing, establishing, and terminating a connection. A firewall with stateful inspection will show the destination IP address and ports. Reviewing the destination IP address will also provide information regarding what is being allowed to pass a DNS response from an external source.
SOURCE: NIST SP 800-41, 2009.
21. **Destination Port Number -** Identifies a service listening on the destination host, and a source port; it usually identifies the port number on the source host that the destination host should reply to. Many transport protocols have ports, but some do not. The combination of the source IP address and the port with destination IP address and port helps define the session. In a sniffer trace, the highest layer represents the end user applications (Layer 7). Based on defined policies, firewalls inspect the application layer traffic and decide what is allowed to pass in or out of the network. A sniffer capture will provide information about how the firewall is handling traffic.
SOURCE: NIST SP 800-41, 2009.

22. **Differentiated Services Code Point (DSCP) -** A means of classifying and managing network traffic and of providing quality of service (QoS) in modern Network Layer 3 IP networks. It uses the 6-bit Differentiated Services (DS) field in the IP header for the purpose of packet classification. Differentiated services (DiffServ) is a computer networking architecture that specifies a simple and scalable mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks.
SOURCE: Dialogic, 2019.
23. **Display Filter -** Used for general packet filtering while viewing for color codes, ruling, and protocols. Display filters can be built to show all packets that contain the TCP protocol.
SOURCE: Wireshark, 2019.
24. **Domain Name Service (DNS) and DNS traffic** - A hierarchy of Internet servers that translate alphanumeric domain names into IP addresses. For example, 172.217.7.164 in place of www.google.com.
SOURCE: Gregg & Santos, 2019.
25. **Eavesdropping -** The unauthorized capture and reading of network traffic or other type of network communication.
SOURCE: Gregg & Santos, 2019.
26. **Echo Reply and Echo Request -** Used by the ping command to test networks. The second part of Internet Control Message Protocol (ICMP) ping, officially a type 0 that is sent in response to an echo request. The echo request is the first part of the ICMP ping, a type 8. Used in protocol analysis to determine the status of a device.
SOURCE: Gregg & Santos, 2019.
27. **eth0 -** When sniffing with tcpdump or Wireshark, this is the Ethernet interface that is configured to display information about the network adapters, such as the IP address and the system name. Listening occurs this interface, eth0.
SOURCE: Carnegie Mellon, 2009.
28. **Ethernet -** This is the Data Link (Layer 2) protocol, which handles communications on the physical network components in LANs and is an IEEE 802.3 standard.
SOURCE: NIST SP 800-41, 2009.
29. **Ethernet Type -** This refers to the type of network and network topology that is being considered when configuring Wireshark and Tcpdump. For example, a hub-based network as compared to a switched network, will determine what traffic will be visible to the sniffer.
SOURCE: Carnegie Mellon University, 2009.
30. **Expressions -** Used in tcpdump, there are three expressions that consist of one or more qualifiers: *type, dir,* and *proto*.
SOURCE: Carnegie Mellon, 2009.
31. **Expressions "Type" -** Option uses host, net, and port. This allows a filter based on addressing/ports with the packet. *Host, net*, and *port* are allowed keywords, and without these the host is assumed. SOURCE: Carnegie Mellon, 2009.

CYBRARY

32. **Expressions "dir" -** Short for direction. Options are *src, dst*, and combinations of these (*src, dst, src or dst, and src* and *dst*). By using *dir*, you can narrow the type to the source or destination field in the packet. If nothing is specified, the *src* or *dst* is assumed by both Wireshark and tcpdump.
    SOURCE: Carnegie Mellon, 2009.
33. **Expression "proto" -** Short for protocol, this option restricts the capture to a specific protocol. Allowed protocols include IP, IPv6, ARP, TCP, and UDP. The options for "proto" are *tcp, udp, icmp, ah,* and etc. If no protocol is specified, all matching protocols in the selected type and direction are displayed or captured.
    SOURCE: Carnegie Mellon, 2009.
34. **Fiber Distributed Data Interface (FDDI)** - A high-speed token-passing technology that employee two rings with traffic closing in opposite direction. FDDI is a legacy infrastructure concept that is mostly replace by SDH and SONET. The sniffer traffic for FDDI will be seen as two bi-directional rings or paths of traffic, traveling is opposite directions.
    SOURCE: Chapple, & Stewart, 2018.
35. **Flag(s) -** Flags are used to select which descriptions to capture in tcpdump or other sniffers. A flag can indicate or dictate which packet to capture or how a packet should be viewed for later analysis. For example, using the -c flag indicates the capturing of packets should be continued. Another example of a flag use, the -A flag can be used to capture web pages.
    SOURCE: Manpage, 2019.
36. **FIN -** Indicates a transmission has "finished" and no additional data packets are forthcoming. In the TCP three-way handshake, the receiver of the original message is the last part to communicate and sends the final FIN when the communication has concluded. SOURCE: KeyCDN, 2018.
37. **Flow/Flow Label -** The combination of a port number and the IP address where connection-orientated (TCP) communication is occurring over Transport Layer 4. It may also include connectionless (UDP) communications (but not at Layer 4). Wireshark labels flows which can be selected for use with the display filter.
    SOURCE: Wireshark, 2019.
38. **Follow TCP Stream -** A function that allows the packets from one TCP stream to be displayed in order, for viewing the stream as it has been received at the Application Layer 7.
    SOURCE: Wireshark, 2019.
39. **File Transfer Protocol (FTP) -** An Internet standard for transferring files over the Internet, usually in cleartext; programs and utilities are used to upload and download web pages, graphics, and other files between local media and remote server with allows FTP access. FTP uses port 20 (data transfer) and port 21 (control, command).
    SOURCE: NIST SP 800-47, 2002.
40. **Fragment/fragment offset -** When a packet exceeds the network interface card (NIC) maximum transmission unit (MTU) value in size, the packet must be broken down into

smaller chunks (fragments) in order for it to be delivered to the destination. At the destination, the fragments are reassembled to form the original packet. The source must send additional information in the IP header for the destination device to be able to reassemble the fragments of the packet into the original order in which it was sent.
SOURCE: Roa & Nayak, 2014.

41. **Fragment Overlap -** This can refer to attack techniques which takes advantage of the reassembly of an authentication header (AH). If a packet is fragmented, it will be discarded to prevent an overlapping fragment attack. This type of attack misuses the fragment assembly algorithm to create and forge packets to force them through the firewall.
SOURCE: Parziale, Britt, Davis, Forrester, Liu, Matthews, & Rosselot, 2006.
42. **Gateway -** An entrance point between networks, this is a network node equipped for interfacing with another network that uses different protocols. In a protocol stream or sniffer capture, it is possible to see communications between devices contained in the gateway, which can be used for network mapping.
SOURCE: Dialogic, 2019.
43. **GET request** - Within HTTP and client browsers, the GET command is used to request data from a specified resource. GET requests can return information such as cache, browser history, and bookmarks. It is a non-harmful command that simply returns information.
SOURCE: W3Schools, 2019.
44. **Hash (key hash) -** A mathematical algorithm used to ensure that a transmitted message has not been tampered with. As a one-way algorithm, it is used to map or translate one set of bits into a fixed length value that can be used to unique identify data.
SOURCE: Gregg & Santos, 2019.
45. **Header Checksum** - A field is a checksum for the information contained in the header; if the header checksum does not match the contents, the datagram is discarded by the intended recipient. The header checksum will then be re-calculated. In IPv4, the checksum filed is required for measuring errors in the header. In IPv6, the checksum field is eliminated from the header.
SOURCES: Parziale, et. al., 2006; and IPwithease, 2019.
46. **Header Length -** IPv4 uses a variable 20-byte; IPv6 uses a fixed 40-byte parameter.
SOURCE: IPwithease, 2019.
47. **HEX -** Short for hexadecimal, this is a base 16 number that is represented in alphanumeric sets, that can be converted to decimal values. In tcpdump, -X telnet options are printed as hex.
SOURCE: Wireshark, 2019.

CYBRARY

48. **Hop (hop count, hop limit, hop-by-hop option) -** This refers to the time it takes data to travel between routers. When used in packet analysis, hop counts provide information on: 1) The time that could be exceeded; 2) The default value that a node has in place in its hop count; and 3) The number of devices through which the data is passing between a source and a destination. Determining the hop count can provide information on the size of the network and or network mapping.
    SOURCE: Parziale, et. al., 2006.
49. **Host Name** - The name of any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means.
    SOURCE: CNSSI No. 2009, 2015.
50. **Internet Control Message Protocol (ICMP) -** Utility that delivers status messages, reports errors, replies to certain request (ICMP echo reply and request), and reports routing information used to test connectivity and troubleshoot problems on IP networks. Used most frequently as the “ping” utility. Can be used in ICMP attacks, which can occur in at least two methods: 1) Mapping the network for vulnerability; and 2) ICMP tunneling in which the attacker inserts data to establish a covert communication channel. A sniffer trace would show a type between 0-41 with a descriptive name (e.g., 0 = echo reply, 8 = echo request).
    SOURCE: Harris & Maymi, 2018.
51. **ICMP Payload -** Refers to an assumption of routers and firewalls to allow ICMP packets into and out of a network because the ICMP was developed to not hold any data or payload. An attack involves adding data to the ICMP request to establish a covert channel and tunneling software, to allow the attacker to listen on a port to identify a back door, to which the attacker could gain access. Essentially, the attacker sends commands inside of ICMP packets; used also to redirect traffic.
    SOURCE: Harris & Maymi, 2018.
52. **Internet Message Access Protocol (IMAP) -** An internet protocol that enables users to access mail on a mail server; similar to POP3 but with more functionality. Messages download to a remote device can be left on the server (in the mailbox).
    SOURCE: Harris & Maymi, 2018.
53. **IP header protocol field value** - An element of an IP packet header that identifies the protocol used in the IP packet payload (usually 6 for TCP, 17 for UDP, and or 1 for ICMP, or any of other valid routing protocol numbers).
    SOURCE: Chapple, et al., 2018.
54. **Message Digest** - The fixed-length bit string produced by a hash function.
    SOURCE: Baker, Chen, & Moody, 2014.
55. **Multicast -** A communications transmission to multiple identified recipients.
    SOURCE: Chappel, et al., 2018.

CYBRARY

56. **Maximum Transmission Unit (MTU)** - The size of the largest datagram that can be sent over a network. If the size exceeds the set limit on the NIC, the packet must be fragmented into smaller datagrams. The MTU size can be seen as an indication of the size of the network where data is being captured. For example, a point-to-point (PPP) network has an MTU of 296 bytes; an IEEE 802.3 network has a default MTU of 1,492 bytes.
    SOURCE: Tech-Faq, 2019.
57. **Open Capture File -** A dialog box used to locate, sort, and view past data captures. The dialog box allows you to select options such as file names, MAC name resolution, network name resolution, transport name resolution, and other ".pcap" files for viewing.
    SOURCE: Wireshark, 2019.
58. **Packet -** The logical unit of network communications produced by the Transport Layer (OSI Layer 4, TCP Layer 4).
    SOURCE: NIST SP 800-86, 2006.
59. **Passive Wiretapping/Passive Sniffing -** The host's network interface is used in promiscuous mode to capture all data in transit, including all packets between hosts, IP addresses, and traffic where hubs are used in the network. Man-in-the-middle (MiTM) attacks use passive sniffing to monitor all traffic, which is then modified to allow the attacker to masquerade as one of the original communicating parties. The main purpose of passive wiretapping is to capture all information entering and leaving the LAN.
    SOURCES: CNSSI 4009, 2015; and Carnegie Mellon, 2009.
60. **Payload -** Information that is concealed and transmitted. SOURCE: Harris & Maymi, 2018.
61. **ping command / ping sweep -** The process of sending ICMP ping request to a series of devices or to the entire range of networked devices.
    SOURCE: Gregg & Santos, 2019.
62. **POP3 -** Post Office Protocol is a protocol used to transfer email messages from an email server to an email client. Sniffing specifically for POP3 is done to view the email authentication packets that are passing over the line, to be able to detect the decodes and the passwords that could be visible if POP3 is unencrypted. Without encrypted email, the sniffer can detect email user names and passwords, the type of email protocol, and the server IP address.
    SOURCES: Chapple, et al., 2018; and SecurityXploded, 2019.
63. **Promiscuous Mode -** Packet sniffers are designed to monitor network traffic on a wired or wireless networks and capture packets. A NIC normally accepts incoming packets but can be set to promiscuous mode, meaning the NIC accepts all incoming packets regardless of the intended destination. When using a sniffer, the sniffer should place the NIC in promiscuous mode, then the user can capture all packets based on the selection of what you desire to view.
    SOURCE: NIST SP 800-86, 2006.

64. **Protocol Analyzer -** Used by packet sniffers to reassemble stream from individual packets and decode communications that use any of hundreds of thousands of different protocols. They can also process live traffic as well as packets that have been previously recored in a capture file. Protocol analyzers are used to display raw packet data in a readable format. SOURCE**:** NIST SP 800-86, 2006.
65. **Putty -** Known also as PuTTY, it is a Windows OS program used for remote access. It is used to record keyboard and mouse inputs, and functions like Telnet or Rlogin. SOURCE: File.net, 2019.
66. **Secure Multipurpose Internet Mail Extensions (S/MIME) -** A protocol used to secure the transmission of email and attachments. SOURCE: Chapple, et. al., 2018.
67. **Session Initiated Protocol (SIP) -** The Internet Engineering Task Force's (IETF's) standard for multimedia conference over IP. It is an ASCII-based, application-layer control protocol that can be used to establish, maintain, and terminate calls between two or more end points. SIP addresses signaling and session management within IP telephony. Signaling allows call information to be carried across networks and session management provides the ability to control the attributes of a call, end to end. SOURCE: IPwithease, 2016.
68. **Simple Mail Transport Protocol (SMTP) Port 25 -** Protocol used for email exchange between clients to servers and between server to server. SOURCE: Chapple, et. al., 2018.
69. **Simple Network Management Protocol (SNMP) -** An application layer protocol that facilitates the exchange of management information between network devices. Version 1 uses well-known community strings of public and private; Version 3 offers encryption. SOURCE: Gregg & Santos, 2019.
70. **Sniffer -** A hardware or software device that can be used to intercept and decode network traffic. SOURCE: Gregg & Santos, 2019.
71. **Secure Shell (SSH) Port 22 -** An end-to-end encryption techniques used for secure remote connection to devices. SOURCE: Chapple, et. al., 2018.
72. **SYN -** Synchronize/start command used to start a normal TCP connection, in which the host receives a SYN packet from a s source hose and sends back a SYN ACK (synchronized acknowledge) packet. SOURCE: Cisco, 2006.
73. **SYN Flood Attack -** A denial of service (DoS) or disturbed denial of service (DDoS) attack in which the attacker sends a successor of SYN packets that never completes the three-way TCP handshake. SOURCE: Harris & Maymi, 2018.

CYBRARY

74. **TCP Stream** - The constant flow of TCP packets across a hard wired or wireless medium. In Wireshark, a TCP stream can be selected to follow through the Wireshark GUI. Tcpdump is an operating system CLI tool that allows you to follow streams of packets from a network interface. Streams are captured at Data Link Layer 4. Data that cannot be read or printed will be represented by dots.
    SOURCE: Wireshark, 2019.
75. **Telnet -** The abbreviated name for teletype network, it is a protocol that uses a command line to access another host. As it does not provide encryption, the protocol poses serious security risks as it can be used by attackers to install malware or viruses on a targeted system, or to extract sensitive information. Uses TCP port 23.
    SOURCE: RFC 855, 1983.
76. **Telnet Session -** Used as a utility to gain remote access to other computing devices installed on a network. The access can be via the Internet or over a closed LAN. To establish a connection, the IP address of the target host will be needed, as well as the username and the password. Telnet sessions are considered unsecured and communications can be captured in cleartext.
    SOURCE: Tech-Faq, 2019.
77. **Time to Live (TTL) -** Used in computing and networking technology, it is units of time or iterations that a transmission occurs before the packet is discarded (prevents endless circulation of a packet). TTL is used by DNS and for DNS caching as set by the name server for each resource record.
    SOURCE: NIST SP 800-21, 2013.
78. **Timestamp -** The time stamps used in Wireshark are generated from the libpcap (Npcap) library, as mandated by the OS kernel. The timestamp format is in time of day in nanoseconds since midnight, and can be reviewed in the “View” menu, under the Time Display Format option.
    SOURCE: Wireshark, 2019.
79. **tos -** The type of service field. SOURCE: Manpage, 2019.
80. **Tunnel -** An IT interconnection component used in creating virtual private networks (VPNs), which is used by two or more parties to communicate security across a public network by creating a private connection or “tunnel” between the two parties. In sniffing, if the VPN is encrypted, the data in transit through the VPN is encrypted and undetectable by the sniffer.
    SOURCE**:** NIST SP 800-47, 2002.
81. **Tunneled Protocols -** Common tunneling protocols that can be viewed via a Wireshark or tcpdump capture include: IPv4, IPv6, Generic Routing Encapsulation (GRE) on port 47, OpenVPN on UPD port 1194, Secure Socket Tunneling Protocol (SSTP) on port 443, Internet Protocol Security (IPsec) on port 50 and 51, Layer 2 Tunneling Protocol (L2TP) on port 115, and Virtual Extensible Local Area Network (VXLAN) on port 4789.
    SOURCE: RFC 2817, 2019.

82. **Unicast -** A communication transmission to a single identified recipient.
    SOURCE: Chapple, et. al., 2018.
83. Urg**ent flag (URG) -** Flag used to notify the receiver to process the urgent packets before processing all other packets. The receiver will be notified when all known urgent data has been received.
    SOURCES**:** RFC 6093, 2011.
84. **Urgent Pointer -** Represented by a “U” or seen as “urg” to indicate a change in the packet, or urgent data is contained within the packet.
    SOURCE: Manpage, 2019.
85. **VLAN -** A virtual LAN is a logical network segmentation on switches and or bridge for the purpose of managing network traffic. Multiple VLANs can be hosted on a single switch or on separate switches for the purpose of isolating network traffic. In sniffing, the viewable traffic from VLANs can be found on the Physical Layer 1, as traffic between devices or over networked segments.
    SOURCE: Chapple, et al., 2018.
86. **Worm -** Malicious, self-replicating code, that works through the system without causing harm to the host but instead infects other systems for the purpose of information gathering. As worms replicate, they consume bandwidth and can be used for denial of service (DoS) attacks.
    SOURCE: Chapple, et al., 2018.
87. **Wireless Local Area Network (WLAN)** - Group of wireless access points and associated infrastructure within a limited geographic area, that is capable of radio communications. Usually implemented as an extension to existing wired LANs to provide enhanced user mobility.
    SOURCE**:** Chapple, et. al., 2018.

CYBRARY

Section 2. General Commands
(from Wireshark Help File)

-a <capture autostop condition>
-b <capture ring buffer option>
-B <capture buffer size>
-c <capture packet count>
-C <configuration profile>
--display=<X display to use>
-f <capture filter>
-g <packet number>
-i <capture interface>|-
-J <jump filter>
-K <keytab>
-m <font>
-N <name resolving flags>
-o <preference/recent setting>
-P <path setting>
-r <infile>
-R <read (display) filter>
-s <capture snaplen>
-t a|ad|adoy|d|dd|e|r|u|ud|udoy
Set the format of the packet timestamp displayed in the packet list window. The format can be one of:

- **a absolute:** The absolute time, as local time in your time zone, is the actual time the packet was captured, with no date displayed
- **ad absolute with date**: The absolute date, displayed as YYYY-MM-DD, and time, as local time in your time zone, is the actual time and date the packet was captured
- **adoy** absolute with date using day of year: The absolute date, displayed as YYYY/DOY, and time, as local time in your time zone, is the actual time and date the packet was captured
- **d delta:** The delta time is the time since the previous packet was captured

CYBRARY

- **dd delta_displayed:** The delta_displayed time is the time since the previous displayed packet was captured
- **e epoch:** The time in seconds since epoch (Jan 1, 1970 00:00:00)
- **r relative:** The relative time is the time elapsed between the first packet and the current packet
- **u UTC:** The absolute time, as UTC, is the actual time the packet was captured, with no date displayed
- **ud UTC with date**: The absolute date, displayed as YYYY-MM-DD, and time, as UTC, is the actual time and date the packet was captured
- **udoy UTC with date using day of year:** The absolute date, displayed as YYYY/DOY, and time, as UTC, is the actual time and date the packet was captured. The default format is relative.

-w <outfile>
-X <eXtension options>
-y <capture link type>
-Y <displaY filter>
-z <statistics>
-z help
-z afp,srt[,filter]
-z conv,type[,filter]
-z dcerpc,srt,name-or-uuid,major.minor[,filter]
-z bootp,stat[,filter]
-z expert
-z fc,srt[,filter]
-z h225,counter[,filter]
-z h225,srt[,filter]
-z io,stat
-z megaco,srt[,filter]
-z mgcp,srt[,filter]
-z mtp3,msus[,<filter>]
-z multicast,stat[,<filter>]
-z rpc,programs

CYBRARY

Section 3. Acronyms

ADS	Alternate Data Stream
AH	Authentication Header
ALG	Application Layer Gateways
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
CA	Certificate Authority
CIDR	Classless Inter-Domain Routing CPU Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone DNS Domain Name System DoS Denial of Service
DNS	Domain Name System
ESP	Encapsulating Security Payload
FAT	File Allocation Table
FTP	File Transfer Protocol
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ID	Identification
IDE	Integrated Drive Electronics
IDS	Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IPsec	Internet Protocol Security
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security

CYBRARY

IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IRC	Internet Relay Chat
IRQ	Interrupt Request Line
ISP	Internet Service Provider
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MD	Message Digest
MIME	Multipurpose Internet Mail Extensions
NAC	Network Access Control
NAP	Network Access Protection
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NFS	Network File Sharing
NIC	Network Interface Card
NTFS	Windows NT File System
NTP	Network Time Protocol
PAT	Port Address Translation
PMTU	Path Maximum Transmission Unit
POP	Post Office Protocol
RADIUS	Remote Authentication Dial In User Service
SFTP	Secure FTP
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol

CYBRARY

TLS	Transport Layer Security
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
UTM	Unified Threat Management
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extensible Markup Language

CYBRARY

Reference

(n.d.). *ASCII Table*. Retrieved August 11, 2019 from: http://www.asciitable.com

(2019). Computer Security Resource Center (CSRC). *Information Technology Laboratory, National Institute of Standards and Technology (NIST).* Retrieved August 11, 2019 from: https://csrc.nist.gov/glossary/term/American-Standard-Code-for-Information-Interchange

Carnegie Mellon. (2009). Packet sniffing with Wireshark and Tcpdump, v.1.1. CERT Training and Education. School of Science, Hampton University. *Publication by Carnegie Mellon University.* Retrieved August 15, 2019 from: https://science.hamptonu.edu/compsci/docs/iac/packet_sniffing.pdf

Chapple, M., Stewart, J.M., & Gibson, D. (2018). Glossary for the CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, 8th Edition. *Sybex.* John Wiley & Sons, Inc., Indianapolis, Indiana. Retrieved from Apple iBooks.

Cisco. (2006, January 6). Defining strategies to protect against TCP SYN denial of service attacks. Document ID: 14760. *Cisco.* Retrieved August 13, 2019 from: https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/14760-4.html?dtid=osscdc000283

Ibid. (2009). Bridge ID Clarification. *The Cisco Learning Network.* Retrieved August 11, 2019 from: https://learningnetwork.cisco.com/thread/5465

CNSSI No. 2009. (2015, April 6th). Committee on National Security Systems (CNSS) Glossary. *Recommendations from The National Security Agency (NSA).* Retrieved August 2, 2019 from: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

CYBRARY

Fisher, T. (2019, May 16). What is Fragmentation and defragmentation? *Lifewire.* Retrieved August 13, 2019 from: https://www.lifewire.com/what-is-fragmentation-defragmentation-2625884

Gregg, M., & Santos, O. (2019). Cert Guide, Certified Ethical Hacker (CEH) Version 10., Third Edition. *Pearson's Education, Inc.* ISBN: 9780135305409. Accessed August 13, 2019 at O'Reilly learning on line. https://www.oreilly.com/online-learning/

Harris, S., & Maymi, F. (2018). All in One CISSP Exam Guide, 8th Ed., *McGraw Hill Education.* New York, NY. Retrieved from Apple iBook conversion by Code Mantra.

Jones, G., & Butterworth, A. (2015, Aug. 15). 1722 AVTP Audio Format. *Apple, Inc.* Retrieved August 2, 2019 from; http://grouper.ieee.org/groups/1722/contributions/2011/butterworth-1722a-avtp-audio-format.pdf

Lane, K., (2018, May 1). What is the advanced message queuing protocol (AMQP)? Integration Zone. *DZone, online*. Retrieved August 13, 2019 from: https://dzone.com/articles/what-is-the-advanced-message-queuing-protocol-amqp

Parziale, L., Britt, D., Davis, C., Forrester, J., Liu, W., Matthews, C. & Rosselot, N. (2006, Dec. 19). TCP/IP Tutorial and Technical Overview, *IMB Redbooks.* IBM Corp., North Castle Dr., Armonk, NY. ISBN-10: 0738494682. Retrieved August 14, 2019 from Apple iBooks.

Roa, U. H., & Nayak, U. (2014). The InfoSec Handbook. An introduction to information security. *Apress Media, LLC.* Retrieved August 14, 2019 from: Apple iBooks.

CYBRARY

NIST SP Reference

[800-38F] Dworkin, M., (2012, Dec.). NIST SP 800-38F, Recommendation for block cipher modes of operation: Methods for key wrapping. Recommendations of the National Institute of Standards and Technology. Retrieved August 12, 2019 from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf

[800-41] Scarfone, K., & Hoffman, P. (2009, Sept.). NISTP SP 800-41, Rev. 1, Guidelines on firewalls and firewall policy. Recommendations of the National Institute of Standards and Technology. Retrieved August 14, 2019 from: https://doi.org/10.6028/NIST.SP.800-41

[800-47] Grance, T., Hash, J., Peck, S., Smith, J., & Korow-Diks, K. (2002, August). NIST SP 800-47, Security guide for interconnecting information technology systems. Recommendations form the National Institutes of Standards and Technology (NIST). Retrieved August 15, 2019 from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-47.pdf

[800-56B] Baker, E., Chen, L., & Moody, D. (2014, Sept.). NIST SP 800-56B, Rev. 1, Recommendation for pair-wise Key establishment schemes using integer factorization cryptography. Retrieved August 13, 2019 from: http://dx.doi.org/10.6028/NIST.SP.800-56Br1

[800-21] Chandramouli, R., & Rose, S. (2013, Sept.). NIST SP 800-81-2, Secure domain name system (DNS) deployment guide. Recommendations from the National Institute of Standards and Technology. Retrieved August 15, 2019 from: http://dx.doi.org/10.6028/NIST.SP.800-81-2

[800-82] Stouffer, K., Pillitteri, V., Abrams, M., & Hahn, A. (2015, May). NIST SP 800-82, Revision 2, Guide to industrial control system (ICS) security; Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and other control systems such a Programmable Logic Controllers (PLC). Retrieved August 11, 2019 from: http://dx.doi.org/10.6028/NIST.SP.800-82r2

[800-86] Kent, K., Chevalier, S., Grance, T., and Dang, H. (2006, August). NIST SP 800-86, Guide to integrating forensic techniques into incident response. Recommendations of the National Institute of Standards and Technology. Retrieved August 11, 2019 from: https://doi.org/10.6028/NIST.SP.800-86

[800-128] Johnson, A., Dempsey, K., Ross, R., Gupta, S. & Bailey, D. (2011, August). NIST SP 800-128, Guide for security-focused configuration management of information systems. Recommendations of the National Institute of Standards and Technology. Retrieved August 11, 2019 from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-128.pdf

RFC Resources

[RFC 855] (1983, May). Telnet Option Specifications. Working Group. Recommendations from the Internet Engineering Task Force (ITEF). Retrieved from: https://tools.ietf.org/html/rfc855

[RFC 2817] (2019). Upgrading to TLS within HTTP/1.1, IETF Datatracker. Retrieved August 15, 2019 from: https://datatracker.ietf.org/doc/rfc2817/

[RFC 6093] Gont, F., & Yourtchenko, A. (2011, Jan.). RFC 6093. On the implementation of the TCP urgent mechanism. Internet Engineering Task Force (IETF). Retrieved August 13, 2019 from: https://tools.ietf.org/html/rfc6093

Web Resources

The Free Dictionary. (2003.) The Free On-line Dictionary of Computing. *DECnet.* Retrieved August 13 2019 from https://encyclopedia2.thefreedictionary.com/DECnet

EC-Council. (2018). CEH. *EC-Council.* Retrieved August 13, 2019 from: https://cert.eccouncil.org/certified-ethical-hacker.html

IPWITHEASE. (2016, November, 24). SIP vs H323. *IPWITHEASE.* Retrieved August 14, 2019 from: https://ipwithease.com/sip-vs-h323/

KeyCDN. (2018, Oct. 4). TCP Flags. *KeyCDN*. Retrieved August 13, 2019 from: https://www.lifewire.com/what-is-fragmentation-defragmentation-2625884

Manpage. (2019). Manpage of TCPDUMP. Retrieved August 15, 2018 from: https://datatracker.ietf.org/doc/rfc2817/

Dialogic. (2019). Differentiated services code point. Dialogic Glossary. *Dialogic Corporation.* Retrieved August 13, 2019 from: https://www.dialogic.com/glossary/differentiated-services-code-point-dscp

Ibid. (2019). Gateway. *Dialogic Corporation.* Retrieved August 13, 2019 from: https://www.dialogic.com/glossary/gateway

File.Net. (2019). What is putty.exe? *File.Net,* (2019). Retrieved August 14, 2019 from: https://www.file.net/process/putty.exe.html

SecurityXploded. (2019). Mail password sniffer. *SecurityXploded, online.* Retrieved August 14, 2019 from: https://securityxploded.com/mail-password-sniffer.php

Tech-Faq. (2019). Maximum Transmission Unit (MTU). Tech-Faq. Retrieved August 15, 2019 from: http://www.tech-faq.com/mtu.html

W3schools. (2019). HTTP request methods. *W3schools online.* Retrieved August 14, 2019 from: https://www.w3schools.com/tags/ref_httpmethods.asp

Wireshark. (2019). Wireshark docs. Retrieved August 14, 2019 from: https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html

Ibid. Chapter 7 Advanced Topics, Section 7.2. Following protocol streams. https://www.wireshark.org/docs/wsug_html_chunked/ChAdvFollowStreamSection.html

Ibid. (2019). Chapter 6. Working with captured packets; Section 6.4. Building display filter expressions. Retrieved August 12, 2019 from: https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html