Bowie Seniors Computer Club

Meeting Minutes for Meeting of March 21, 2019

Attendees: Bill Alli, Carl Bulger, Joan Dubbs, Sam Duff, Dennis Evans, Dale Grant, Margaret Gregory, Barry Hammond, Eric Hein, Dick Henthorn, Berry Hill, Janice Holland, James Kozura, Steve Krulik, Dan Lee, Bill Long, Bill Macri, Tom McCabe, Bob Rapczynski, Irv Salzberg, Dan Searing, Flo Strawser. Visitor: Karen Dorondo

Carl Bulger opened the meeting at 12:35. Dan Lee told of upcoming meeting programs: (April 4, 2019 - Mr. Larry Hudson, a local realtor, April 18, 2019 - Mr. Christopher Barber, Chief Nerd, Cheaperthanageek, May 2, 2019 - Mr. Neil Bloomberg.)

Bill Macri gave a presentation on the Wireshark network packet analysis application. A copy of his Powerpoint slides is attached. The presentation included an online demonstration and discussion of how Wireshark can be used to hack packet information. Because Wireshark is a tool used by hackers this led to a subsequent discussion on computer safety. Bill stated that we should have multiple email accounts and use guest accounts to separate important correspondence from non-important correspondence. Also use free or paid Malwarebytes for malware protection (Bob Blum questioned whether Malwarebytes is a Russian Kasperski application). Bill passed around a credit-card like device that is used by hackers for surreptitious downloads (see photo).

There was a a discussion of how to deal with PUPs (Potentially Unwanted Programs). Bill Long noted that magazines ***PCWorld*** and ***PCMagazine*** are available free online from public AACPL library and that one of them recently tested various antivirus applications and found Microsoft's Defender to be the best for Ransomware protection.

Eric Hein described a situation in which you will not be able to boot a computer from a USB device. If a computer is a UEFI computer (not one with the older BIOS) and had been shutdown with its Fast Startup setting enabled, it will not boot from a USB device. This is because shutting down with Fast Startup enabled puts a computer in Hibernate mode rather than Shutdown mode. UEFI systems cannot boot from a USB device when in Hibernate mode.

Bill Long advised members that when shutting down a desktop computer for a long

period of time listen closely to the system enclosure to hear if any fans are running inside. Power supply fans and processor cooling fans if running will continue to bring dust into the system.

Bill Long, Secretary

Computer Security Rehash

All Computers

BIOS - Old

Basic Input / Output System

UEFI - New

Unified Extensible Firmware Interface

(safe boot)


You Have Been Hacked

Internal

Log On

Main – Admin rights

Personal

Guest – Local rights : No system updates

Grandkids

local user

Anti-Virus

EXAMPLES

- ACTIVE
  - Norton
  - MacAfee
  - Windows Defender
- CLEANER
  - Malwarebytes (Free Version)

Paid vs Free

Paid

- Annual Subscription
- Stop paying – stops updating
- 1 800 support 24/7

Free

- Continues to update
- “No” 1 800 support (depends)

Malware Access

- Internal
  - Games
  - Email
  - USB sticks
- External
  - Cloud
  - Cable
  - Browser

Email Addresses

- Multiple Email Addresses
  - Suggestions
    - Personal
    - Online Shopping
    - Online Inquires

IE Demo

External

Wireless Monitoring

Examples

- Solar Winds
- Manage Engine OP Manager
- Paessler PRTG Network Monitor
- Wireshark

- See
  - https://www.comparitech.com/net-admin/network-monitoring-tools/

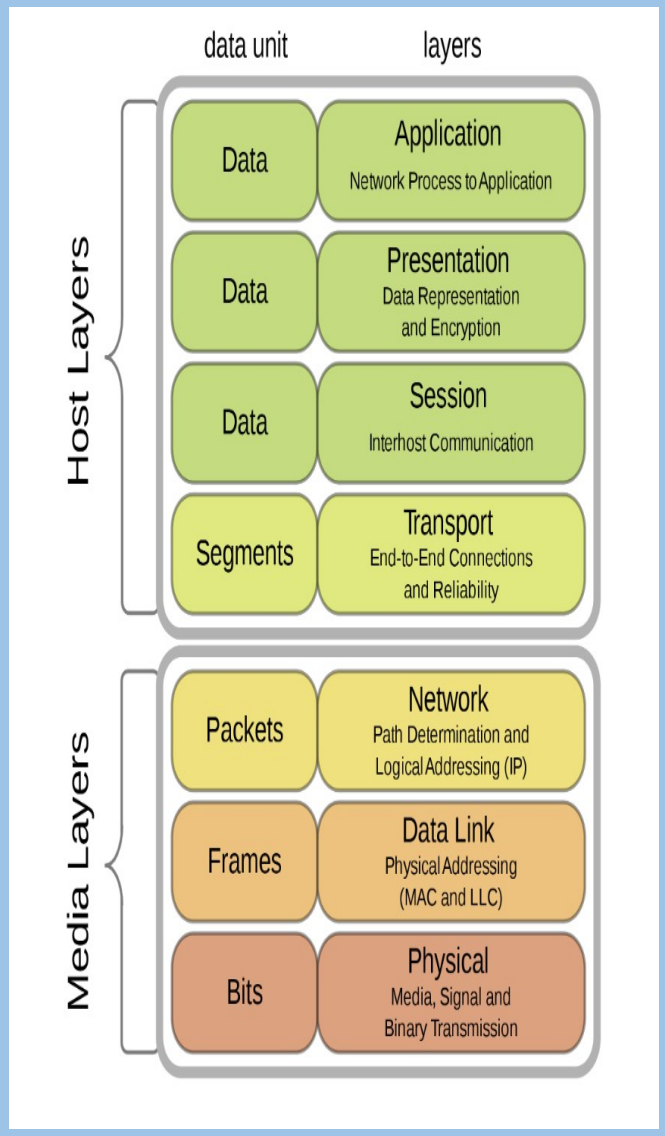
WIRESHARK

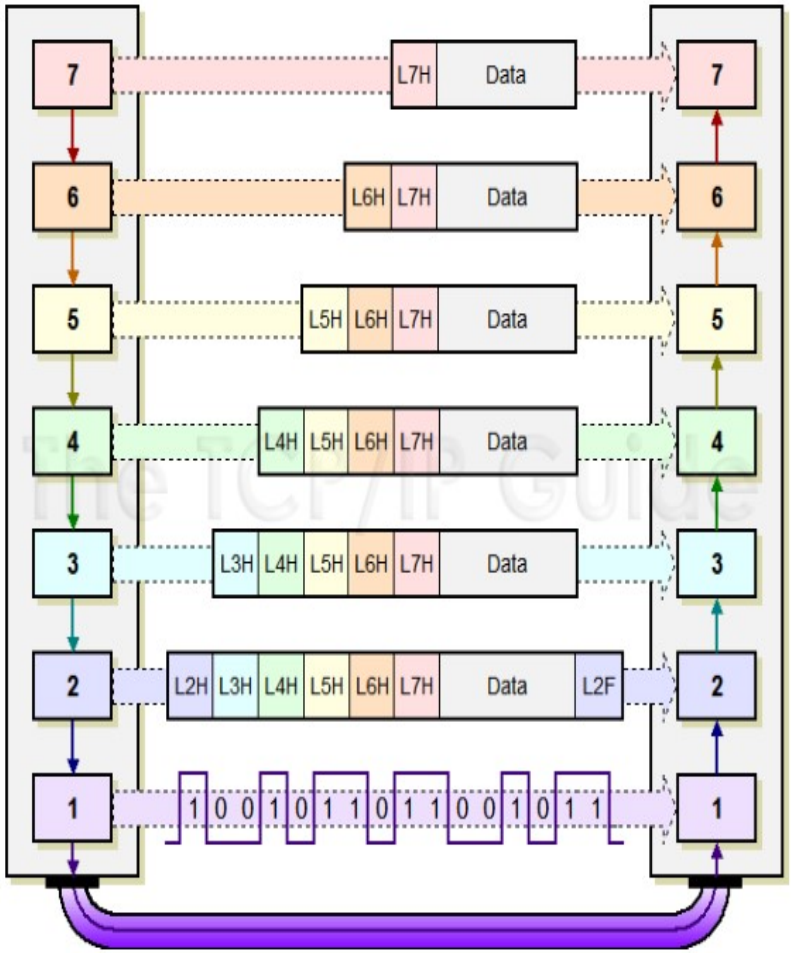
Wireshark

- *Wireshark* is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible ...

Features

- Wireshark has a rich feature set which includes the following:
- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- **Multi-platform: Runs on Windows, Linux, OS X, FreeBSD, NetBSD, and many others**
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- The most powerful display filters in the industry
- Rich VoIP analysis
- Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, and many others
- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- ***Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2***
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript®, CSV, or plain text


data unit
layers
Host Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Media Layers
Packets
Network
Path Determination and Logical Addressing (IP)
Frames
Data Link
Physical Addressing (MAC and LLC)
Bits
Physical
Media, Signal and Binary Transmission


7
6
5
4
3
2
1
L7H
Data
L6H
L5H
L4H
L3H
L2H
L2F
1 0 0 1 0 1 1 0 1 1 0 0 1 0 1 1

Ports

- Port numbers relate to network addressing. In TCP/IP networking, both TCP and UDP use their own set of ports that work together with IP addresses.
- These port numbers work like telephone extensions. Just as a business telephone switchboard can use the main phone number and assign each employee an extension number (like x100, x101, etc.), so too can a computer have a main address and a set of port numbers to handle incoming and outgoing connections.
- In the same way that one phone number can be used for all the employees within that building, one IP address can be used to communicate with various kinds of applications behind one router; the IP address identifies the destination computer and the port

Ports

Ports

- 0 – 65535 – TCP
- 0 – 65535 – UDP

0 – 1024 Reserved

Netstat –abno (admin)

Common Ports (reserved)

- 20: File Transfer Protocol (FTP) Data Transfer
- 21: File Transfer Protocol (FTP) Command Control
- 22: Secure Shell (SSH) Secure Login
- 23: Telnet remote login service, unencrypted text messages
- 25: Simple Mail Transfer Protocol (SMTP) E-mail routing
- 53: Domain Name System (DNS) service
- 80: Hypertext Transfer Protocol (HTTP) used in the World Wide Web
- 110: Post Office Protocol (POP3)
- 119: Network News Transfer Protocol (NNTP)
- 123: Network Time Protocol (NTP)
- 143: Internet Message Access Protocol (IMAP) Management of digital mail
- 161: Simple Network Management Protocol (SNMP)
- 194: Internet Relay Chat (IRC)
- 443: HTTP Secure (HTTPS) HTTP over TLS/SSL

www.shutterstock.com • 1124997365

WIRESHARK DEMO