CHRIST
(DEEMED TO BE UNIVERSITY)
BANGALORE · INDIA

Department of Computer Science and Engineering

Computer Society of India

Presents

Workshop

On

WIRESHARK

Scan to Register

Venue
Room No 218, First Floor, Second Block,
Kengeri Campus.

Event Coordinator : Dr. Jayapandian N (jayapandian.n@christuniversity.in)

Department Vision: " To Fortify Ethical Computational Excellence"


CHRIST
Computer Society of India
Workshop on
Date : 10.02.2020
WIRESHARK

Department of Computer Science and Engineering
Computer Society of India

Event Report

Workshop
On
WIRESHARK

CONDUCTED BY : COMPUTER SOCIETY OF INDIA
DATE & TIME : 14TH FEB, 2020. 4:30-6:00 PM
VENUE : #218, 2ND BLOCK, CHRIST - KENGERI CAMPUS
RESOURCE PERSONS: ARIYAN JAIN & MAYANK JALANIA
EVENT COORDINATOR: Dr JAYAPANDIAN N.
Total No. of Participants: 27

Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is the default standard across many industries and educational institutions.

Wireshark development thrives thanks to the contributions of networking experts across the globe. It is the continuation of a project that started in 1998.

CSI student Body of School of Engineering and Technology, Christ (Deemed to be University), took this initiative to reach out to student community of institute to introduce Wireshark and help the students to become industry ready.

Workshop was attended by more than 25 enthusiastic students. Every attendee was happy with the resource persons and were satisfied with the knowledge gained.

Trainers explained about the features & Funcationality of wireshark.

Features includes:

- 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)

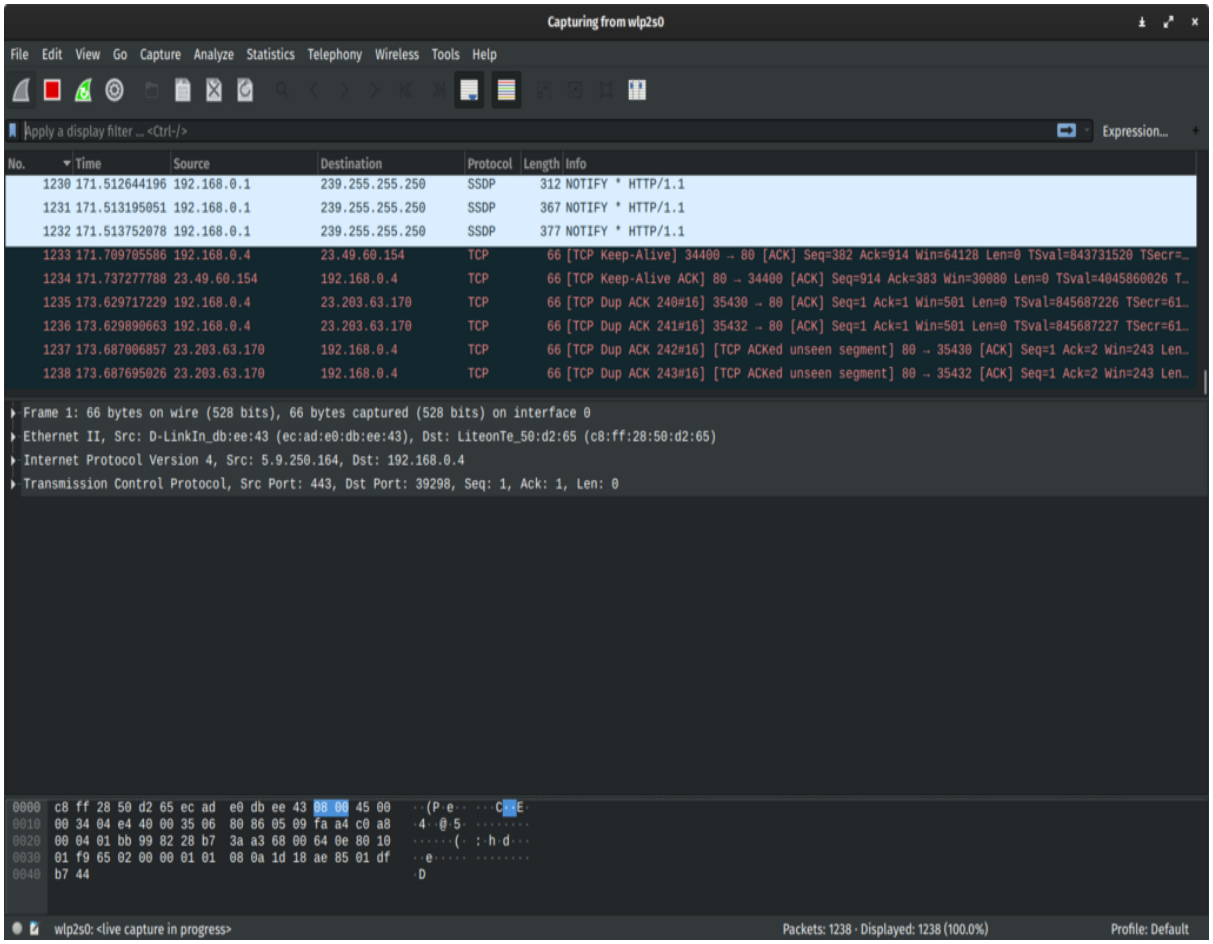
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript®, CSV, or plain text

Functionality Includes:

Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

Wireshark lets the user put network interface controllers into promiscuous mode (if supported by the network interface controller), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's MAC address. However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic. Port mirroring or various network taps extend capture to any point on the network. Simple passive taps are extremely resistant to tampering. On GNU/Linux, BSD, and macOS, with libpcap 1.0.0 or later, Wireshark 1.4 and later can also put wireless network interface controllers into monitor mode.

If a remote machine captures packets and sends the captured packets to a machine running Wireshark using the TZSP protocol or the protocol used by OmniPeek, Wireshark dissects those packets, so it can analyze packets captured on a remote machine at the time that they are captured.



Overall the workshop was a huge success. It has provided the attendees a great exposure. It will definitely help each one of us to get Industry ready. It has also helped some students to start some research projects in the domain.

Head of the Department
Computer Science and Engineering
CHRIST (Deemed to be University)
Bengaluru - 560 074

Workshop on

WireShark

Computer Society of India & Department of CSE

CHRIST (Deemed to be University), Bangalore-560074, India

14th Feb 2020

S.NO	Name of the Participants	Signature
1	Allam Vineth Reddy [1760474]	
2	Sai Chandra Reddy [1760456]	
3	B. Devi Shivani [1861033]	
4	S. Reema Sree [1860455]	
5	P. Sai Mahesh [1861008]	
6	P. Dharma Deepak [1860348]	
7	Yashwanth [1860438]	
8	Chris S Peter [1860433]	
9	Nirmal Rajesh [1860434]	
10	K.V.S. Bhavya Sree [1861016]	
11	Vyshnavi. S.B [1860453]	
12	ABIN ASU (1860301)	
13	Kasania Sachin Kapil (1860335)	
14	Avvavajjala Abhiram Sai (1760661)	
15	Bhavana. P (1860633)	
16	Salman Masood (1760432)	
17	M. Gopi Chandu (1961436)	
18	Rahul Raj Dixit [1860350]	
19	JOE CHIRAKKEKARAN [1860047]	
20	TIYA ANN SIBY [1861020]	

Workshop on

WireShark

Computer Society of India & Department of CSE

CHRIST (Deemed to be University), Bangalore-560074, India

14th Feb 2020

S.NO	Name of the Participants	Signature
21	Chinthala Sreya Reddy (1860386)	
22	SOURADIP TAH. 1960479	
23	ALFIYA K C 1760380	
24	Danish Thomas 1860317	
25	Jerin Philip 1860327	
26	T. Vijay Kumar 1860416	
27	Sahaush Pamecha (1860424)	