

UC.yber; Meeting 24

Meet New Leadership and Wireshark

If You're New!

- Join our Slack **ucyber.slack.com**
- Follow us on **Twitter @UCyb3r** and Facebook UC.yber; University of Cincinnati OWASP Chapter
- Feel free to get involved with one of our committees: **Content, Finance, Public Affairs, Outreach, Recruitment**
- Stay updated through our weekly emails and SLACK



Announcements

- **UC has \$85,000** to spend on equipment
- **Siemens** has the server **ready to pick up**
- **Northrop Grumman** has given us **\$1,000** for a competition team
- **P&G** is ready to bring us on a tour of their **cyber defense center**
- **October 27/28th ACM** programming challenge



Rules Of Engagement (ROE)

- Always operate within the bounds of the law
- Never attack without **written** permission from the target
- Alert any vulnerabilities found to the owner
 - Owner of IP with vulnerability
- Cyber Range is fair Game for attacks





Meet the Committee's

Recruitment and Retention Committee

- Mission Statement: To recruit members in UC.yber and help keep these members interested and engaged by staying in touch with them.
- Get the word out.
- Logo, tshirts, other ways to be recognized
- Survey
- Any other ideas contact me on slack in a private message.



Public Affairs Committee

- Mission Statement: To ensure that the public is informed about the organization's activities and about the priorities and policies of UC.yber;
- Social Media is the key to inform the public (Twitter, Facebook, and Instagram..)
- Lots of collaboration with the Outreach Committee



Public Affairs - Rules of Engagement (ROE)

- Talk to me about post ideas and give me links, the source, or etc.(through Slack or in-person)
- Explain and give reason on why you want the idea to be posted
- If you want to tell someone in person, tell everyone!
- This is more of the creative side of the organization. If anyone is creative and wants to help make flyers, logos, or anything of the sort.. this is the committee you want to be on!



Public Affairs - Goals

- Tell people about our social media accounts and get followers
- Let as many people know about UC.yber; as you can (The more people who know about us, the more opportunities we'll have as an organization)
- End Goal: Get a following and have people know about us



Funding and Finance Committee

- Mission Statement:
 - **To obtain and manage the funds in order to support the chapter.**
 - How?
 - Making connections with companies, and inviting them to be sponsors of our group.
 - Collaborate with the event committee and set up fundraising events.
- Who is involved?
 - Anyone interested in being apart a fundraising event is welcome.



Outreach Committee

- Mission Statement: To plan and organize events in support of the chapter.
- Develop leadership and planning skills within the members of the committee.
- Document outreach activities and preparation for them



Content and Information committee

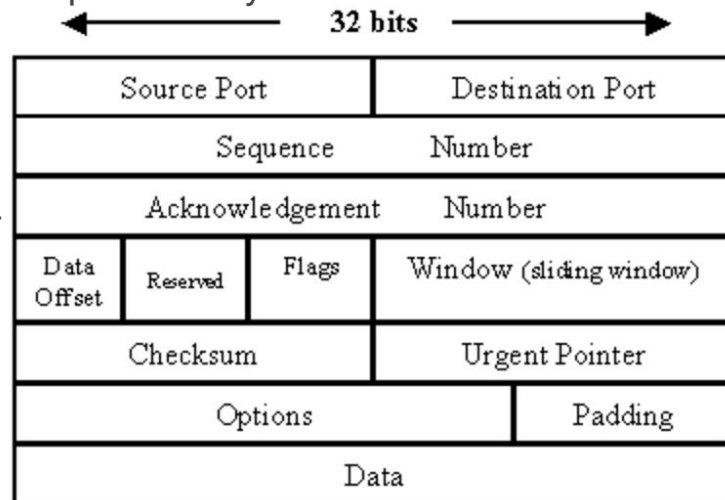
- Mission statement: To educate the members of UC.yber;
- Weekly info sessions.
- Making a repository of the data we collect.
- Providing resources.



Wireshark Tutorial

What's the use?

- Captures network traffic in the form of a **PCAP** file
- PCAP - **P**acket **C**apture
- What is a **packet**?
 - A chunk of data enclosed in one or more wrappers that help to identify the chunk of data and route it to the correct destination
 - Organized by protocol
- What is a **protocol**?
 - A *protocol* is a set of rules governing communications.
 - Ex. **ICMP** for **emails**

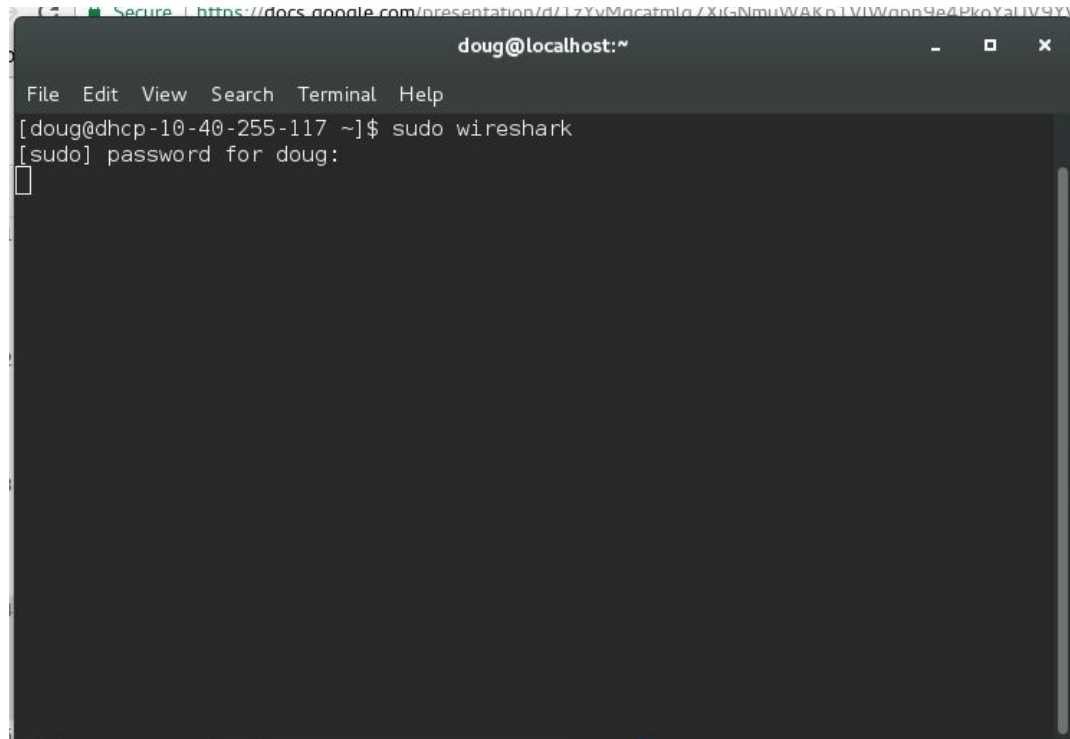


Wireshark Tutorial: Download

- Go to <https://www.wireshark.org> and download correct version



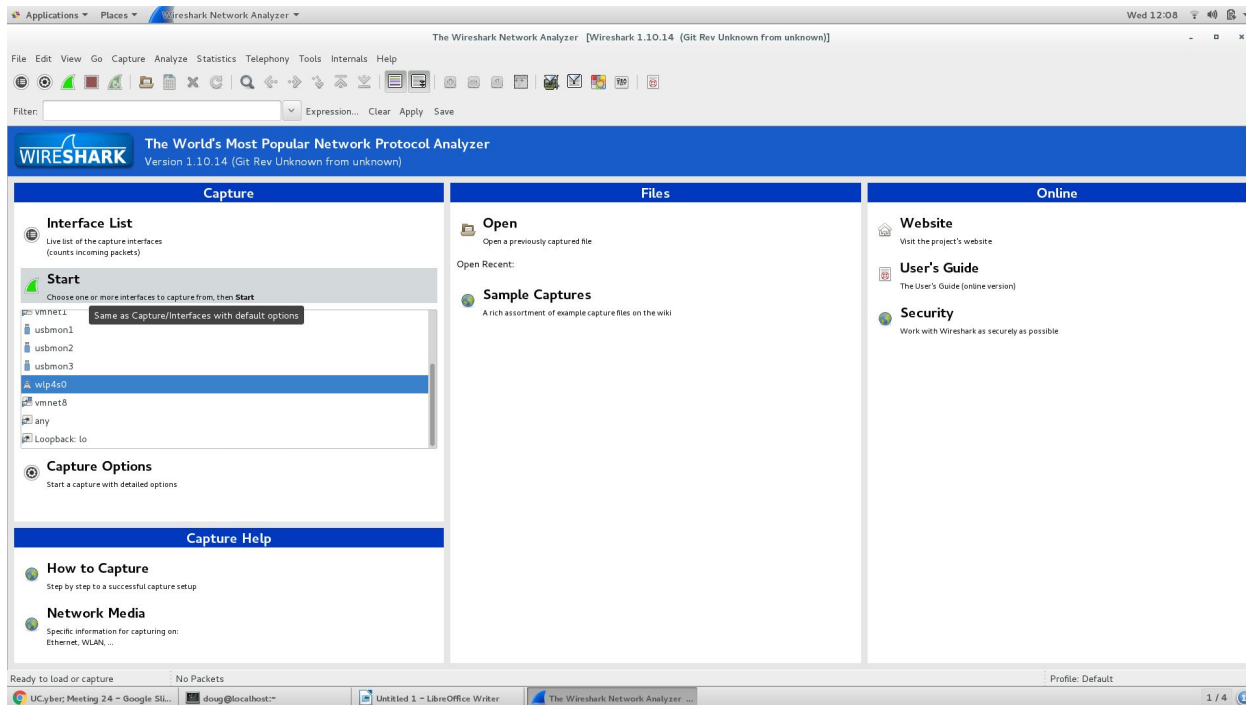
Wireshark Tutorial: Starting Wireshark



A terminal window titled "doug@localhost:~" is shown. The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal content shows the command `[doug@dhcp-10-40-255-117 ~]$ sudo wireshark` being entered. Below this, the prompt `[sudo] password for doug:` is displayed, followed by a small white cursor box indicating where the password should be entered. The terminal window is overlaid on a background that features a Google Docs document viewer at the top and a decorative pink and purple geometric pattern at the bottom right.

```
doug@localhost:~  
File Edit View Search Terminal Help  
[doug@dhcp-10-40-255-117 ~]$ sudo wireshark  
[sudo] password for doug:  
█
```


Wireshark: User Interface



Wireshark: Packet Sniffing

The screenshot displays the Wireshark Network Analyzer interface. The top status bar indicates "Capturing from wlp4s0 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]" and the date "Wed 12:08". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains icons for various functions like opening files, saving, and filtering. The filter field is empty, and the "Expression..." button is visible. The packet list pane shows a table of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 43) is a TCP ACK from 10.40.255.117 to 34.203.14.16. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
34	22.38863004	173.194.198.189	10.40.255.117	UDP	75	Source port: https Destination port: https
35	22.44732057	173.194.198.189	10.40.255.117	UDP	239	Source port: https Destination port: https
36	22.488862102	173.194.198.189	10.40.255.117	UDP	81	Source port: https Destination port: https
37	22.488897373	173.194.198.189	10.40.255.117	UDP	84	Source port: https Destination port: https
38	22.489072374	10.40.255.117	173.194.198.189	UDP	129	Application Data
39	23.121395508	10.40.255.117	34.203.14.16	TLSv1.2	129	Application Data
40	23.141775903	34.203.14.16	10.40.255.117	TLSv1.2	129	Application Data
41	23.141831812	10.40.255.117	34.203.14.16	TCP	66	43580 > https [ACK] Seq=190 Ack=130 Win=493 Len=0 TSval=12690021 TSecr=2256572402
42	30.208055738	10.40.255.117	52.112.64.28	TCP	66	43806 > https [ACK] Seq=1 Ack=1 Win=682 Len=0 TSval=12697088 TSecr=65214105
43	30.242597866	52.112.64.28	10.40.255.117	TCP	66	[TCP ACKed unseen segment] https > 43808 [ACK] Seq=1 Ack=2 Win=253 Len=0 TSval=8218611 TSecr=1260884
44	33.121712833	10.40.255.117	34.203.14.16	TLSv1.2	129	Application Data
45	33.143677967	34.203.14.16	10.40.255.117	TLSv1.2	129	Application Data
46	33.145723171	10.40.255.117	34.203.14.16	TCP	66	43580 > https [ACK] Seq=253 Ack=253 Win=493 Len=0 TSval=12700023 TSecr=2256574902
47	35.766723837	10.40.255.117	64.233.168.94	UDP	1392	Source port: 46611 Destination port: https
48	35.767287795	10.40.255.117	64.233.168.94	UDP	630	Source port: 46611 Destination port: https
49	35.804997832	64.233.168.94	10.40.255.117	UDP	1392	Source port: https Destination port: 46611
50	35.804961302	64.233.168.94	10.40.255.117	UDP	73	Source port: https Destination port: 46611
51	35.805359597	64.233.168.94	10.40.255.117	UDP	72	Source port: https Destination port: 46611
52	35.805610707	10.40.255.117	64.233.168.94	UDP	83	Source port: 46611 Destination port: https
53	35.805728559	10.40.255.117	64.233.168.94	UDP	80	Source port: 46611 Destination port: https
54	35.833860858	64.233.168.94	10.40.255.117	UDP	246	Source port: https Destination port: 46611
55	35.833973309	64.233.168.94	10.40.255.117	UDP	60	Source port: https Destination port: 46611
56	35.834089561	10.40.255.117	64.233.168.94	UDP	83	Source port: 46611 Destination port: https
57	35.863971172	64.233.168.94	10.40.255.117	UDP	72	Source port: https Destination port: 46611

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Ethernet II, Src: IntelCor_44:30:bd (60:57:18:44:30:bd), Dst: Cisco_46:c7:7f (f8:c2:88:46:c7:7f)
- Internet Protocol Version 4, Src: 10.40.255.117 (10.40.255.117), Dst: 108.177.112.188 (108.177.112.188)
- Transmission Control Protocol, Src Port: 46166 (46166), Dst Port: hpvroom (5228), Seq: 1, Ack: 1, Len: 0

```
0000 f8 c2 88 46 c7 7f 60 57 18 44 30 bd 08 00 45 00 ...F..W..00...E.
0010 00 34 7a de 40 00 06 08 da 0a 28 ff 75 6c b1 .4z.e.0. ...(.u.
0020 70 bc b4 56 14 6c f8 19 31 5f aa 9f f8 cc 90 10 p..V.L.L. l.....
0030 00 f5 1e a8 00 01 01 08 0a 00 c1 48 00 36 7a ..... ..W.6c
0040 56 f1
```

Wireshark: Targeting IPs

The image shows the Wireshark Network Analyzer interface. The top menu bar includes Applications, Places, and Wireshark Network Analyzer. The status bar at the top right shows 'Wed 12:11' and 'Capturing from wlp4s0 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]'. The main toolbar contains icons for file operations, capture, analysis, and display. The filter bar at the top of the packet list shows the filter: `ip.src == 216.58.216.100 || ip.dst == 216.58.216.100`. The packet list displays a series of ICMP Echo (ping) requests and replies between 216.58.216.100 and 10.40.255.117. The selected packet (No. 241) is an ICMP Echo (ping) request from 10.40.255.117 to 216.58.216.100. The packet details pane shows the following structure:

- Frame 241: 96 bytes on wire (784 bits), 96 bytes captured (784 bits) on interface 0
- Ethernet II, Src: Cisco_46:c7:7f, Dst: IntelCor_44:30:bd (60:57:18:44:30:bd)
- Internet Protocol Version 4, Src: 216.58.216.100 (216.58.216.100), Dst: 10.40.255.117 (10.40.255.117)
- Internet Control Message Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII format:

```
0000 60 57 18 44 30 bd f8 c2 88 46 c7 7f 08 00 45 00  \V.D0... .F....E.
0010 00 54 00 00 00 00 33 01 cd c6 d8 3a d8 64 0a 28  .T...3. .!..d.(
0020 ff 75 00 00 23 c9 98 16 00 09 45 1d b0 59 00 00  ..#.8. ....f.
0030 00 00 41 cd 0a 00 00 00 00 11 12 13 14 15 00 00  .A.....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .... *%#%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  & (!*... ./012345
0060 36 37 67
```

The status bar at the bottom shows the capture progress: 'wlp4s0: <live capture in progress> F... Packets: 636 - Displayed: 36 (5.7%)'. The bottom toolbar includes icons for file operations, capture, analysis, and display.