CTF Skills - Networking Wireshark, Netcat & Nmap

presented by Mandy Galante, NJCCIC Education Outreach Services
New Jersey Cybersecurity and Communications Integration Cell

Welcome! During the workshop:

- Please use Q&A for questions
- Please use Chat for whole group chat topics
- If you will be following along, start up your VM + log into CyberStart Game & PicoCTF Gym

Workshop Info - Networking

Capture The Flag (CTF) competitions for CyberStart NCS and PicoCTF are coming up soon with opportunities for NJ students to shine and win prizes. Let's get ready! NJCCIC workshops will cover how to use key tools that the experts recommend for solving many CTF challenges.

- The files listed below are needed to follow the workshop demonstrations / slides. You can download them from this link http://bit.ly/NetFiles
- An active CyberStart Game license is necessary to access the CSGame challenges.

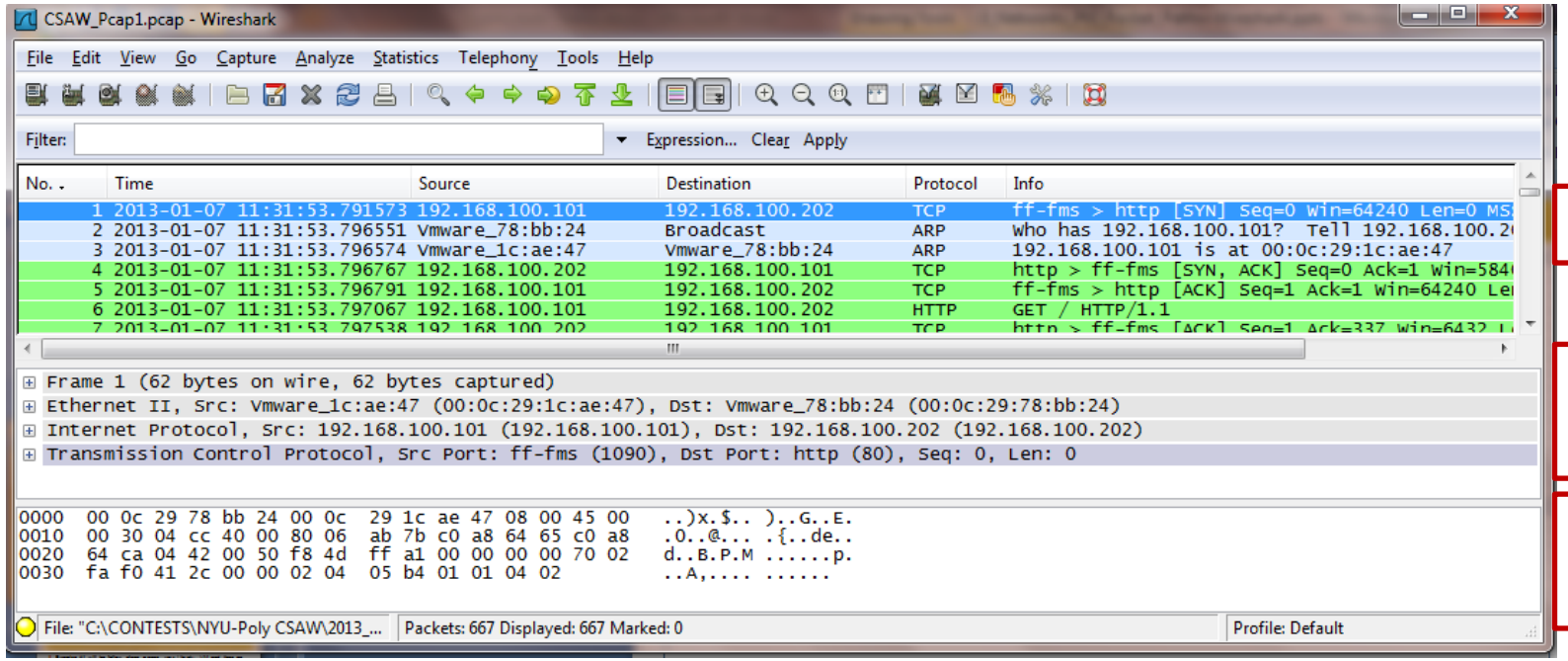
WIRESHARK

Wireshark is a *network packet analyzer (*aka – a *protocol analyzer)*

It captures packets and makes it possible for the user to examine all parts of that packet, including:

*IP address info * Protocols and ports *Actual data from inside the packet

Wireshark has three sections to use for pcap analysis:



1 Packet List

2 Packet Details

3 Packet Bytes

Wireshark

The **Packet List** section gives a chronological list of every packet captured. Includes time, source & destination IP addresses, Protocol and very basic Info

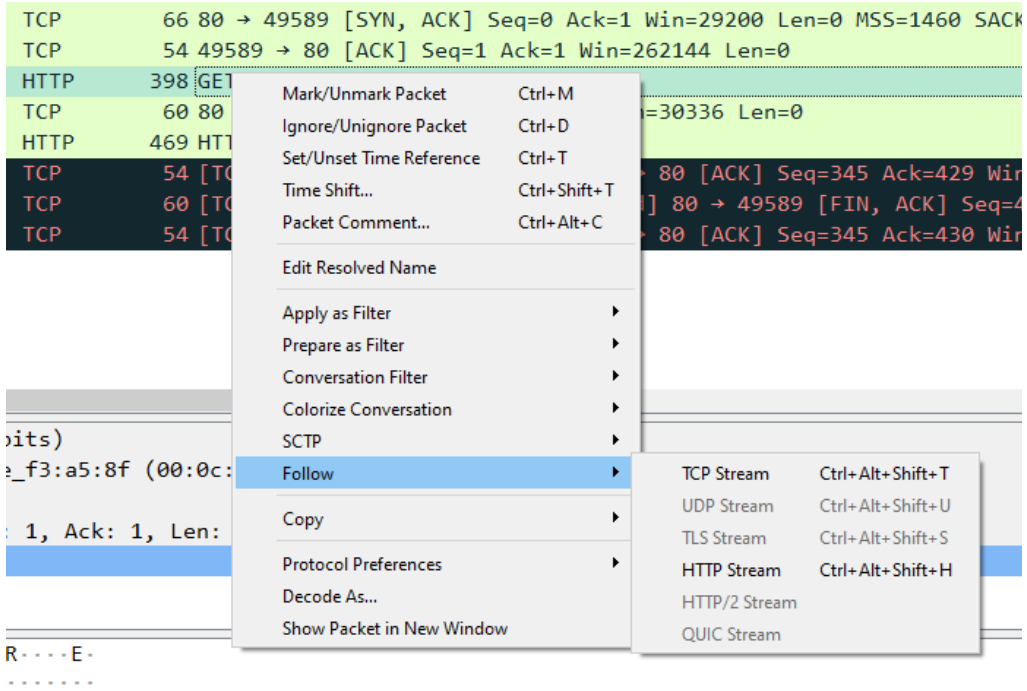
The **Packet Details** section gives more specific info about each packet, grouping the info by the layers of the packet. Here we can find MAC addresses, ports numbers, flags and some text data.

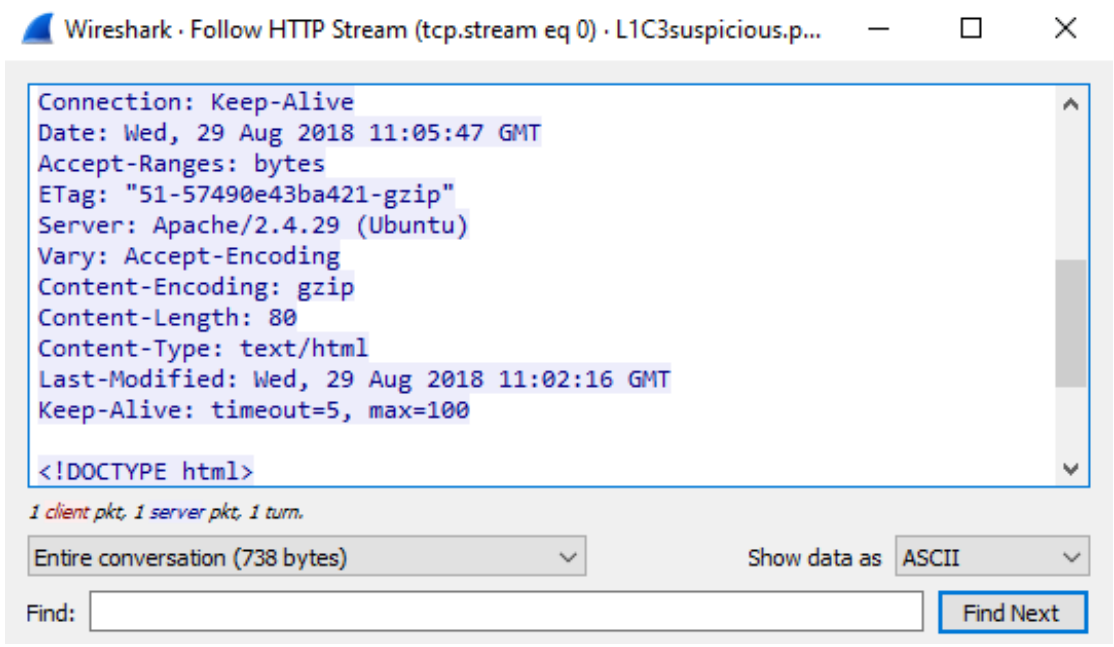
The **Packet Bytes** section shows the data that was carried in the packet. The data is shown in hexadecimal (middle) and text (right).

Pcap files are the older version, newer versions are **pcapng**. Wireshark will open both automatically when you doubleclick.

Wireshark

For certain types of protocols like HTTP, Wireshark will gather up all the packets from a message and display it in human readable form. This is called “following a stream”. Rightclick on a packet and select Follow | <select available stream>





This creates a filter so make sure to click X in the green bar or Clear at top when done with this stream

CyberStart - Forensics:L1C3 Wireshark

Briefing: One of the things our agents did while in the field was to get a packet capture from the suspected employee's computer for us to analyze. Can you take a look and fill in page one of the forensics report we're preparing for the client.

Tip: Analyze the packet capture to get the right information to put in the report.

File: suspicious.pcap -- I renamed to L1C3suspicious.pcap

Hint: Check out a tool called Wireshark, it can help you follow the 'HTTP stream'.

Report Questions:

Was the connection successful or unsuccessful? SYN - SYN/ACK - ACK

What was the status code? HTTP Status codes

What is the flag seen in the data transfer? Right click on HTTP packet - follow HTTP

PicoGym: Shark on Wire 1 Wireshark

Description: We found this packet capture. Recover the flag.

Hints: Use Wireshark & What are streams?

---

1. Search usually won't help in a CTF but you should try it. Select the Search icon, select Strings and enter *pico* or *CTF* or *{*
2. Find which packets transferred data -- on the top toolbar click Statistics | Protocol Hierarchy | under Internet Protocol V4 find the Data line & rightclick
   | Select as Apply as Filter | Selected
   -- click Close
3. Investigate those packets

Walkthrough video solutions for all PicoGym challenges:
https://www.youtube.com/user/carlislemc/playlists

CyberStart - Forensics:L3C4 Wireshark

Briefing: As part of our work helping the New York branch, we took on the task of monitoring some of the sites the hackers have been looking at - one of which was a job board for graphic designers. We managed to get a network capture of one of them viewing a job posting which we suspect has a secret message in it. See if you can confirm that by looking at this pcap (packet capture) file.

Tip: The flag is in the file.

File: job board suspicious packets.pcapng-- I renamed to L3C4job_board.pcapng

Hint: Have you tried using a tool called 'Wireshark'? It has a follow stream option which can be helpful in identifying traffic. There's also an option to find specific packets. Perhaps try searching for the string "flag" and see would you find.

CyberStart - Forensics:L3C4 Wireshark

Search for flag as per hint - find packet that says “Yes this is where you are supposed to be” AND we can see “flag “in data bytes pane

Note: Wireshark grabs any files that came with the packets including text, pictures, html, icons from websites - everything! And you can download a copy of any of those files.

go to File |Export Objects | HTTP → explore the list of files

select a file | at the bottom click Save| give name and save
(If on Windows, make sure to put the right extension on the filename)

PicoGym:What's a NetCat? Netcat

Briefing:. Using netcat (nc) is going to be pretty important. Can you connect to **jupiter.challenges.picoctf.org** at port **25103** to get the flag?

The **Netcat** tool is used to easily connect to another device. It can be used to exchange messages and data.

Syntax:

connect = `nc <ip or name of destination> <port #>`

Example: **`nc 192.168.1.1 5678`** **`or nc services@cybergame.com 5678`**

CyberStart - HQ:7-2 NetCat

Briefing: We have come across a site, which we believe is run by one of the Chiquitoo gang members, that sends information out on the port 1337. We've got a terminal tool you can use that is restricted to do just what you need. See if you can use it to get the information so we can find out what the site is being used for.

Tip: Get the information to get the flag.

Hint: Netcat can be used to listen on a port. Type nc -h to see how to run the command.

listen = `nc -l -p <port #>`

Example: **`nc -l -p 5678`**

CyberStart - HQ:11-12 Nmap & Netcat

Briefing: Quick job for you Agent. We think the gang have a port running between 14000 and 15000 that might expose some interesting information about them, we've temporarily pointed our domain services.cyberprotection.agency to their server. Use that address to find the service and connect to it.

Tip: Connect to the port to get the flag.

Hint: You'll want to use nmap for this. Make sure you specify the port range!

Plan

1. use nmap to scan the network and find which port is open on the target.
2. use netcat to connect to that port.

What's Nmap? 

Nmap

Tool to scan networks and devices. Can be used to send test packets to devices to identify:

- which devices are on - “host discovery scan” or “ping scan”
  Ex: sudo nmap -v -sn 192.168.1.0/24
- what ports the devices have open - “port scan”
  Ex: sudo nmap -v -sS jupiter.challenge.org -p 12000-13500
- what operating system and services are running on the device
  Ex: sudo nmap - v -O 192.168.1.1
- and much more!

```
sudo nmap -v -sS services.cyberprotection.agency -p 14000-15000
sudo nc services.cyberprotection.agency <portnumber>
```

CyberStart - Forensics:L8C4 Wireshark

Briefing: To help expand the investigation we've been permitted to do some analysis on the machines of other dealers that weren't under suspicion of being involved, and we've already found something interesting. Take a look at this network capture, an initial analysis has revealed that it might have some hidden messages in it, can you help us figure out what they are?

Tip: The flag is in the message.

File: wraw.pcapng-- I renamed to L8C4wraw.pcapng

Hint: Raw!

CyberStart - Forensics:L8C4 Wireshark

Plan:

1. Use Statistics | Protocol Hierarchy to filter for the packets with data
2. Follow the TCP Stream to find the right message
3. Save the message as RAW to the VM Downloads folder as ‘Rawfile
4. In terminal, cd to the Downloads folder and use the ‘file Rawfile’ command. This will show what is the format of Rawfile.
5. Open the file to get info about the flag.

Connect With Us

NJCCIC@CYBER.NJ.GOV

1-833-4-NJCCIC
(1-833-465-2242)

@NJCYBERSECURITY

CYBER.NJ.GOV