



## Activity 4

# Denial-of-Service Attack Simulation and Analysis

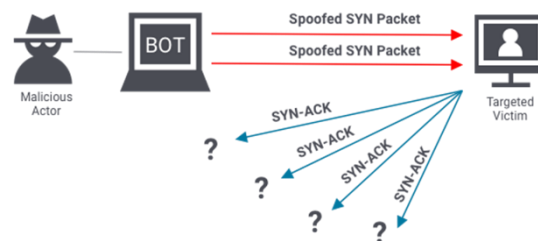
Using various virtual machines, be able to perform “Denial-of-Service Attack Simulation and Analysis” for possible targeted virtualized machines in the network. Also conduct a thorough analysis of a captured network traffic.

### Activity Resources

Virtual Machines: Kali Linux, Ubuntu, Metasploitable

Network Traffic Capture: [Activity4]NetCapture\_Scenario

Tools: Nmap or ZenMap, Wireshark, hping3, Slowloris



*Disclaimer: Activity is for educational purpose only! Misuse or targeting other services outside the controlled or virtual environment is punishable by law and the University. The University and the Instructor has no liability on misuse of the tools used in this exercise.*

### Activity Procedure(s)

#### Task 1 – Denial-of-Service Attack Simulation

In your workstation, open/run Oracle VirtualBox Manager and configure virtual machines (Kali Linux, Ubuntu and Metasploitable) network adapter using the following configurations:

##### Adapter No. 1 Network Configurations

- Enable Network Adapter: YES (checked)
- Attached to: Host-Only Adapter
- Name: Virtual Host-Only Ethernet Adapter (note: choose network that is DHCP server enabled)
- Promiscuous Mode (Advanced): Deny
- Reset MAC Address (press the refresh button)

Run/Start virtual machine simultaneously (make sure all virtual machines are loaded and running). In your Kali Linux virtual machine, perform Network Scanning and Reconnaissance using Nmap or ZenMap tools to identify possible vulnerable target machines (Metasploitable). Next, perform any TCP Flood attack (DoS) technique on the target machine using Hping3 or Slowloris tool. While performing the attack, run Wireshark in Kali Linux to capture the network packet (observe and analyze the results). Also, in your Ubuntu virtual machine, open a browser and access the website hosted by the targeted webserver. Finally, observe and analyze the captured network traffic in Wireshark.

#### Task 2 – Network Traffic Examination and Analysis

Open Wireshark and load the network capture file ([Activity4]NetCapture\_Scenario). Perform the necessary network investigation of the captured network traffic using various examination techniques (filtering, statistics analysis, and expert information analysis).

### Submission Note (Individual Activity)

Use file name convention (LASTNAME\_CTAINASL\_SECTION\_TERM\_AY\_Activity4.pdf).

Submit/upload Softcopy (PDF file) in MS Teams

Submit a PRINTED activity rubric.



# ACTIVITY DOCUMENTATION

Group Name Ctrl+Z

Tuesday, April 22, 2025

Members Surname, First Name MI. (Alphabetical)

Cano, Kaide M.

Cuenca, Sophia T.

Dionela, Terrence A.

Umengan, Darwin F.

Click or tap here to enter text.

Instruction(s): Provide the appropriate screenshot/screen capture of your workstation.

## Network Scanning and Enumeration Simulation

### Nmap/ZenMap Report

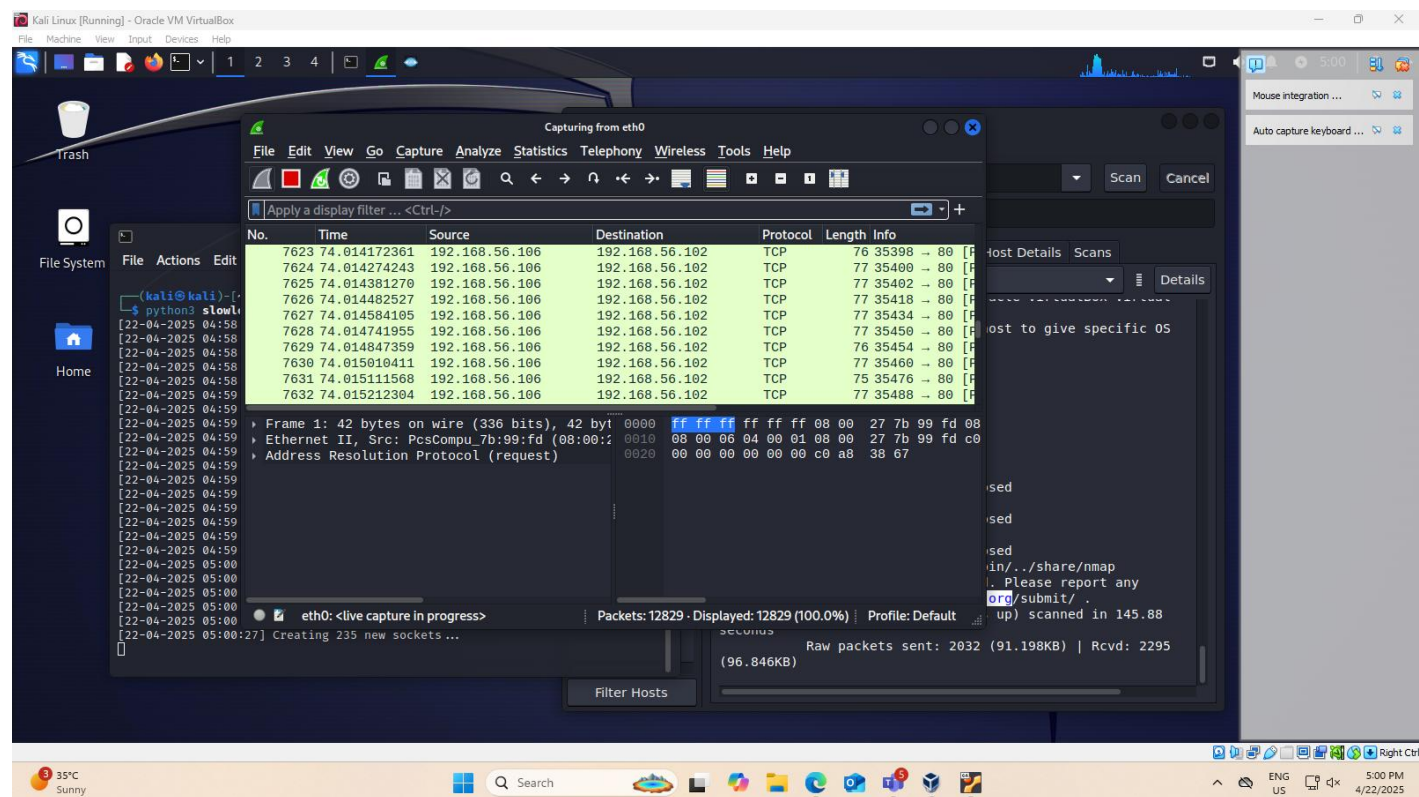
Display here the result of the Nmap/ZenMap report.

The screenshot shows a Kali Linux virtual machine environment. The Zenmap application is running, displaying a scan of the target IP range 192.168.56.102-104. The scan results show that the target host is up and has several open ports. The terminal window shows the execution of a script named 'slowloris' which is attacking the target with 500 sockets. The Zenmap output shows the following discovered open ports:

Port	Protocol	State
22	TCP	Open
139	TCP	Open
445	TCP	Open
3389	TCP	Open
3306	TCP	Open
135	TCP	Open
80	TCP	Open
8080	TCP	Open
8181	TCP	Open
49154	TCP	Open
3000	TCP	Open
8383	TCP	Open
4848	TCP	Open
49156	TCP	Open
49152	TCP	Open
7676	TCP	Open
49153	TCP	Open
8009	TCP	Open
9200	TCP	Open

## Wireshark Report

Display here the result of the captured network traffic using Wireshark.



Q1. What is/are the IP Address of the attacker machine(s) in the network?

[Answer Format: IP Address, ..., IP Address]

Answer: 192.168.56.104

Q2. What is/are the IP Address of the target machine(s) in the network? [Hint: Except machines in ignored states]

[Answer Format: IP Address, ..., IP Address]

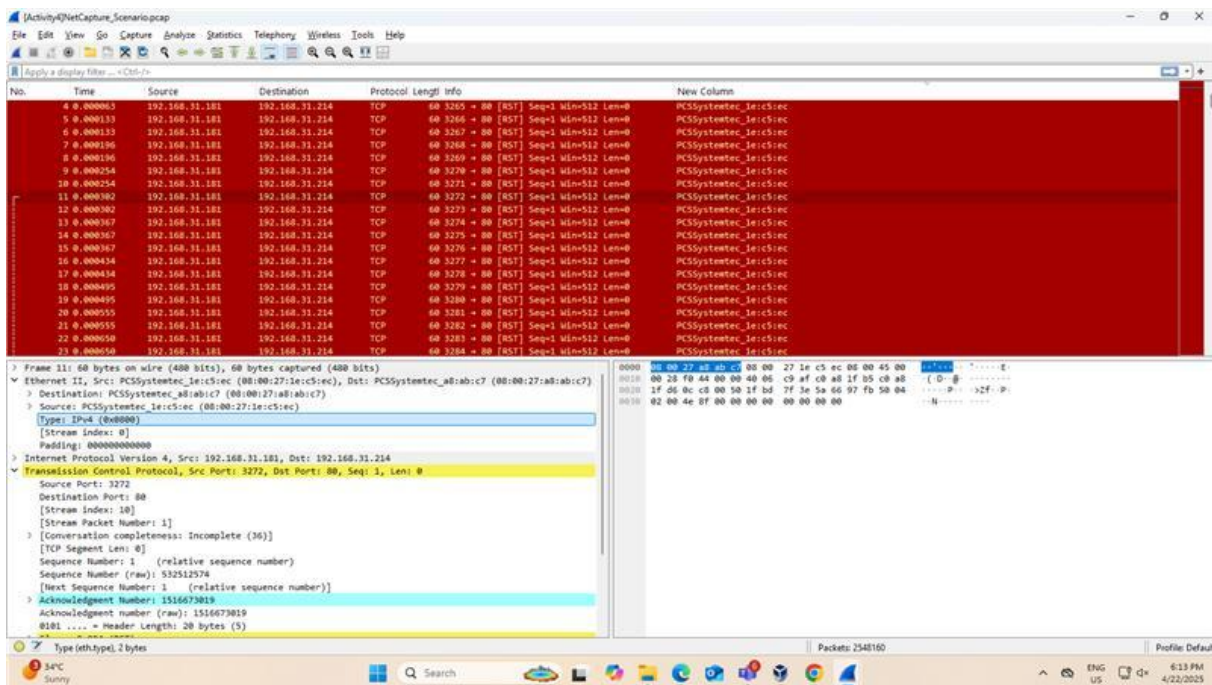
Answer: 192.168.56.102



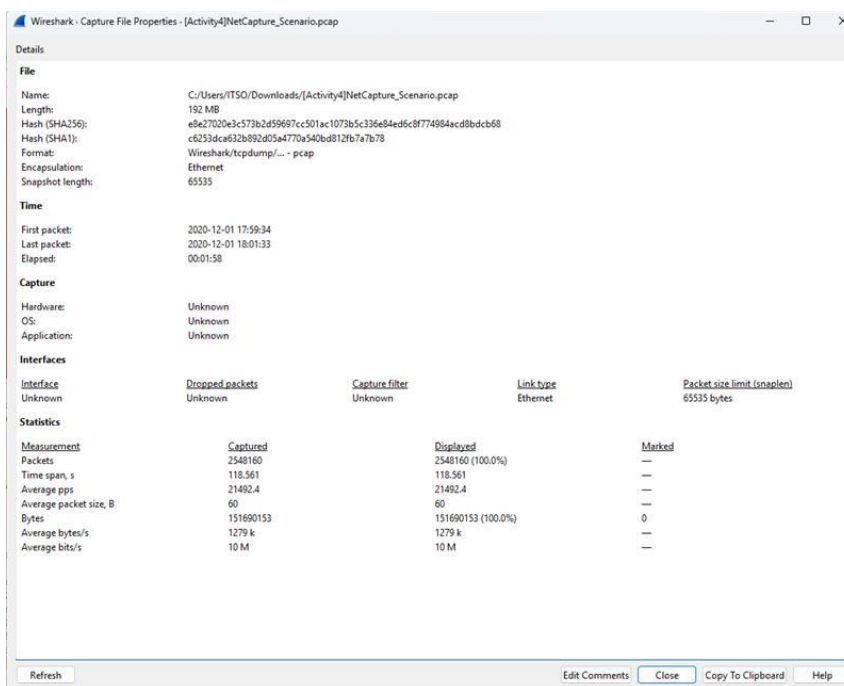
## Network Traffic Examination and Analysis

### Wireshark Capture

Display here the Wireshark capture file.



Display here the Wireshark capture file properties information.







## Wireshark Filtering

Display here the result of the Wireshark capture using various Denial-of-Service detection filter commands.

The screenshot shows a Wireshark capture of network traffic. The packet list pane displays a series of TCP RST (Reset) packets. The source IP address is 192.168.31.181, and the destination IP address is 192.168.31.214. The sequence numbers range from 3265 to 3284. The packet details pane shows the structure of a TCP RST packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol fields. The packet is identified as a TCP RST packet with sequence number 3272 and length 0.

Observation and Findings: What do the filter result suggest? Explain!

Click or tap here to enter text.



## Wireshark Statistics (IPv4 Conversations)

Display here the statistics report.

Wireshark - Conversations - [Activity4]NetCapture\_Scenario.pcap

Conversation Settings

☐ Name resolution

☐ Absolute start time

☐ Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

☐ Bluetooth

☐ BPPv7

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☒ IPv4

☒ IPv6

☐ IPX

☐ JXTA

☐ LTP

Filter list for specific type

Ethernet - 9

IPv4 - 19

IPv6 - 2

TCP - 65550

UDP - 20

Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
23.96.112.38	192.168.31.219	2	209 bytes	17	1	149 bytes	1	60 bytes	95.202161	0.0403	29 kbps	11 kbps
52.41.198.156	192.168.31.109	3	234 bytes	5	2	145 bytes	1	89 bytes	22.117845	0.2397	4839 bits/s	2970 bits/s
52.114.14.165	192.168.31.219	9	2 kB	6	6	1 kB	3	723 bytes	23.052969	80.1896	134 bits/s	72 bits/s
192.168.31.109	172.217.31.238	13	936 bytes	11	7	510 bytes	6	426 bytes	40.514906	54.2727	75 bits/s	62 bits/s
192.168.31.109	192.168.31.1	8	937 bytes	7	4	348 bytes	4	589 bytes	23.141768	36.9054	75 bits/s	127 bits/s
192.168.31.181	192.168.31.214	2,547,716	152 MB	0	2,332,515	140 MB	215,201	12 MB	0.000000	34.5845	15 Mbps	1246 kbps
192.168.31.214	239.255.255.250	12	6 kB	18	12	6 kB	0	0 bytes	117.192250	0.1248	402 kbps	0 bits/s
192.168.31.219	13.107.43.12	20	6 kB	8	9	3 kB	11	3 kB	28.152781	61.5650	372 bits/s	442 bits/s
192.168.31.219	52.38.124.88	7	532 bytes	13	3	240 bytes	4	292 bytes	41.773588	0.8871	2164 bits/s	2633 bits/s
192.168.31.219	52.114.6.177	37	12 kB	3	18	5 kB	19	8 kB	19.648954	61.5576	586 bits/s	983 bits/s
192.168.31.219	52.114.16.91	9	813 bytes	4	6	513 bytes	3	300 bytes	21.854249	80.4057	51 bits/s	29 bits/s
192.168.31.219	52.114.159.32	20	8 kB	16	10	3 kB	10	5 kB	78.799696	1.4025	19 kbps	28 kbps
192.168.31.219	52.139.250.253	6	770 bytes	9	4	314 bytes	2	456 bytes	38.582241	45.0741	55 bits/s	80 bits/s
192.168.31.219	52.218.176.219	38	7 kB	12	19	2 kB	19	5 kB	41.379822	1.3960	12 kbps	28 kbps
192.168.31.219	52.218.232.120	63	14 kB	14	30	4 kB	33	10 kB	43.150837	6.8237	4571 bits/s	12 kbps
192.168.31.219	172.217.161.142	11	777 bytes	15	6	444 bytes	5	333 bytes	51.394295	54.6687	64 bits/s	48 bits/s
192.168.31.219	192.168.31.1	20	2 kB	2	10	889 bytes	10	1 kB	19.640994	39.1582	120 bits/s	197 bits/s
192.168.31.219	192.168.31.255	120	37 kB	1	120	37 kB	0	0 bytes	0.560707	118.0001	2477 bits/s	0 bits/s
192.168.31.219	239.255.255.250	7	5 kB	10	7	5 kB	0	0 bytes	39.061691	5.4137	7220 bits/s	0 bits/s

Close

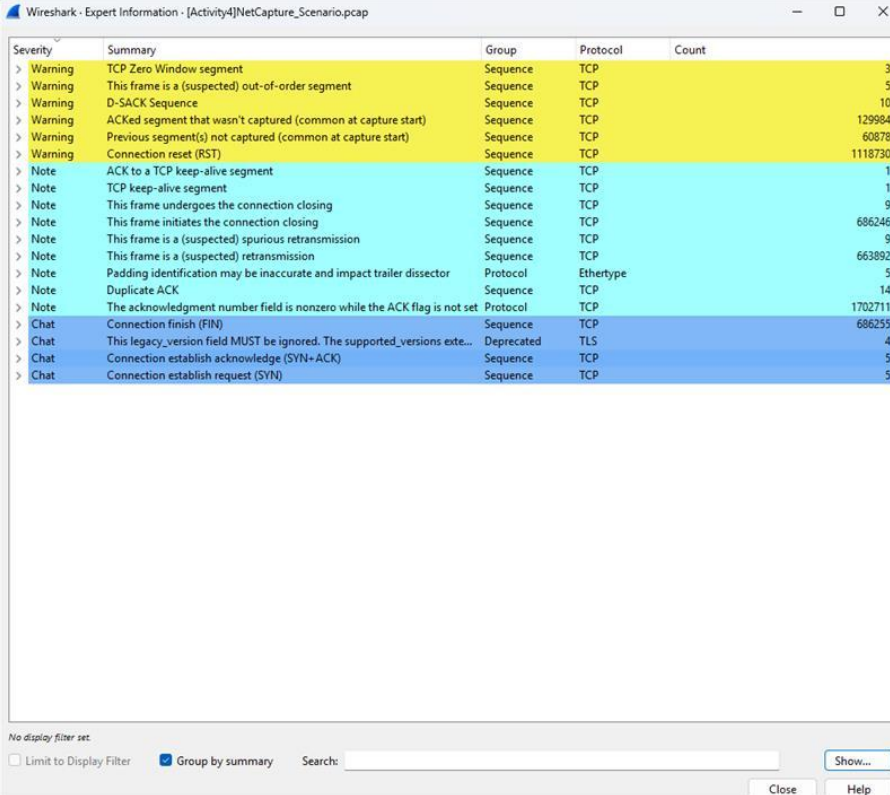
Observation and Findings: What do the statistics result suggest? Explain!

Click or tap here to enter text.



## Wireshark Expert Information

Display here the Expert Information summary report.



Severity	Summary	Group	Protocol	Count
> Warning	TCP Zero Window segment	Sequence	TCP	3
> Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	5
> Warning	D-SACK Sequence	Sequence	TCP	10
> Warning	ACKed segment that wasn't captured (common at capture start)	Sequence	TCP	129984
> Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	60878
> Warning	Connection reset (RST)	Sequence	TCP	1118730
> Note	ACK to a TCP keep-alive segment	Sequence	TCP	1
> Note	TCP keep-alive segment	Sequence	TCP	1
> Note	This frame undergoes the connection closing	Sequence	TCP	9
> Note	This frame initiates the connection closing	Sequence	TCP	686246
> Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	9
> Note	This frame is a (suspected) retransmission	Sequence	TCP	663892
> Note	Padding identification may be inaccurate and impact trailer dissector	Protocol	Ethertype	5
> Note	Duplicate ACK	Sequence	TCP	14
> Note	The acknowledgment number field is nonzero while the ACK flag is not set	Protocol	TCP	1702711
> Chat	Connection finish (FIN)	Sequence	TCP	686255
> Chat	This legacy_version field MUST be ignored. The supported_versions exte...	Deprecated	TLS	4
> Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP	5
> Chat	Connection establish request (SYN)	Sequence	TCP	5

No display filter set.

☐ Limit to Display Filter ☒ Group by summary Search:  Show...

Close Help

Observation and Findings: What do the expert information result suggest? Explain!

Click or tap here to enter text.



### Question and Answer

What is the IP Address of the attacker and the target machine(s) in the captured network traffic?

Answer (Attacker's IP Address) : 192.168.31.181

Answer (Target's IP Address) : 19.168.31.214

What is the MAC Address of the attacker and the target machine(s) in the captured network traffic?

Answer (Attacker's MAC Address) : 08:00:27:1e:c5:ec

Answer (Target's MAC Address) : 80:00:27:a8:ab:c7

What Denial-of-Service attack technique was used by the attacker in the captured network traffic?

Answer: Click or tap here to enter text.

### Mitigation and Recommendations

What are the necessary countermeasures to avoid or prevent Denial-of-Service attacks.

Click or tap here to enter text.





# ACTIVITY RUBRICS

Group Name Click or tap here to enter text.

Tuesday, April 22, 2025

Members Surname, First Name MI. (Alphabetical)

Click or tap here to enter text.

Click or tap here to enter text.

Click or tap here to enter text.

Click or tap here to enter text.

Click or tap here to enter text.

Criteria	Activity Rubrics					Points
	Not Attempted (0 points)	Beginning (1 point)	Developing (2 points)	Proficient (3 points)	Exemplary (4 points)	
Use of Tools & Techniques	No attempt to use relevant tool(s).	Incorrect or unsuitable tool(s) selected.	Tool(s) used is/are somewhat suitable but not optimal.	Selected appropriate tool(s) with minor mismatches to the scenario.	Selected the most appropriate tool(s) for the task based on scenario.	
Execution of Simulation	No attempt to execute attack simulation.	Poorly executed; goals unmet; major safety/ethical concerns.	Execution had flaws; goals only partially met; some safety concerns.	Attack executed with minor issues; met most goals; adhered to safety.	DoS attack executed safely, ethically, and effectively within controlled environment; met all goals.	
Use of Wireshark Filters and Features	No attempt to perform filtering of network traffic data.	Filters not used or configured incorrectly, leading to large irrelevant data.	Basic filters applied; excessive or irrelevant data captured.	Capture filters set up correctly with minor inefficiencies.	Capture filters configured accurately; unnecessary data excluded effectively.	
	No attempt to use Wireshark features.	Wireshark features not used effectively; manual analysis dominates.	Limited use of Wireshark features; investigation hindered by inefficiency.	Basic features used effectively; advanced features used with some errors.	Advanced features used effectively (e.g., filters, color coding, statistics)	
Analysis, Interpretation and Mitigation	No attempt to conduct analysis and interpretation.	Minimal or incorrect analysis; important information overlooked.	Basic analysis performed, but some important findings are missed or misinterpreted.	Results analyzed accurately but with some minor gaps in interpretation.	Detailed and accurate analysis of results; clear identification of open ports, services, and potential vulnerabilities.	
	No attempt to provide recommendations for mitigation.	Incorrect recommendations for mitigation.	Generalized or incomplete recommendations; lacks actionable steps.	Mostly accurate and actionable recommendations with minor omissions.	Accurate and actionable recommendations tailored to the scenario.	
Documentation	No attempt to provide report documentation of findings.	Poor documentation of findings; lacks structure or critical details.	Basic report provided with significant omissions or unclear explanations.	Detailed report provided; minor gaps in methods or findings.	Comprehensive report including methods, findings, and recommendations.	
Total Score and Feedback					TOTAL POINTS EARNED (20 max points)	
<input type="checkbox"/> Exemplary	20	Exemplary work demonstrating mastery of Wireshark features, thorough investigation, analysis, and comprehensive reporting.				
<input type="checkbox"/> Proficient	16-19	Solid performance with minor gaps in technical skills or documentation.				
<input type="checkbox"/> Developing	12-15	Basic understanding of Wireshark and investigation concepts; several significant gaps in execution.				
<input type="checkbox"/> Beginning	8-11	Minimal effort or understanding; critical errors or omissions in the capture, analysis, or reporting.				
<input type="checkbox"/> Not Attempted	0-7	Indicates failure to perform network investigation and analysis.				
Evaluated by:		Remarks/Comments				
Name of Course Instructor						