



Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: Sep 10, 2025	Entry: # 1
Description	Documenting the Security Incident
Tool(s) used	None
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none">● Who caused the incident? An organized group of unethical hackers● What happened? Ransomware Security Incident● When did the incident occur? Tuesday 9.00am● Where did the incident happen? A small U.S. health care clinic● Why did the incident happen? Hackers motivation is money as the ransom note demanded a large sum of money in exchange for the decryption key.
Additional notes	<ul style="list-style-type: none">● How should we prevent a similar kind of incident from the health care company in the future?● Is the company ready to pay in order to retrieve the decryption key?

Date: Sep 12, 2025	Entry: # 2
Description	Packet Capture file
Tool(s) used	Wireshark - it is a network protocol analyzer that uses a graphical user interface
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> • Who caused the incident? - N/A • What happened? - N/A • When did the incident occur? - N/A • Where did the incident happen? - N/A • Why did the incident happen?-N/A
Additional notes	<ul style="list-style-type: none"> • I have not used this WireShark tool before. Seems it is very useful and powerful to analyze the packets over the network.

Date: Sep 15, 2025	Entry: # 3
Description	Capturing my first packet
Tool(s) used	Tcpdump - it is a command line tool for packet analyzer and capture
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> • Who caused the incident? - N/A • What happened? - N/A • When did the incident occur? - N/A • Where did the incident happen?- N/A • Why did the incident happen? - N/A
Additional notes	<ul style="list-style-type: none"> • Got a chance to filter live network packet data from the eth0 interface with tcpdump in this lesson

Date: Sep 18, 2025	Entry: # 4
Description	Investigate a suspicious file hash
Tool(s) used	Virustotal- It is used to analyse suspicious files, domains, IPs and URLs
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> ● Who caused the incident? Unknown malicious actor ● What happened? An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b ● When did the incident occur? An alert was sent to the organization's SOC by 1:20 p.m. ● Where did the incident happen? Employee's computer at a financial services company ● Why did the incident happen? An employee was able to download and execute a malicious file attachment via e-mail.
Additional notes	<ul style="list-style-type: none"> ● Security incident awareness training is important for all employees