Incident handler's journal

Date: Jan.9.2026	**Entry:** #2
Description	Documenting cybersecurity incident considering malicious file
Tool(s) used	Hashing; Using VirusTotal
The 5 W's	• **Who:** Organized group of ethical hackers/Individual hacker • **What happened:** User received email containing attachment, downloaded malicious. • **When: 1:11 PM** • **Where**: Financial services company • **Why**: Incident occurred when user downloaded malicious attachment which he received thru email. User opened file and malicious payload was executed on their computer. At 1:20 p.m. An intrusion detection system detected the executable file and send alert to the SOC. Necessary precautions were made.
Additional notes	Hash value was listed malicious on VrusTotal website by more then 50 vendors.