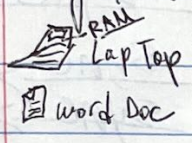
William Prado
08/07/2025

# Digital Forensics

YTB. Overview of a Playbook - incident response
YTB. CISA incident response Playbook
YTB. Digital Forensics Tutorial 3 Digital Forensics Process




Tools
Encase
FTK
"Hash"

YTB. Overview of Digital Forensics
- Identify
- Preserving
- Analyzing
- Presenting Digital Evidence

forensicmag.com
GDI

Legal hold.
Cache memory
System memory
write blocker
Chain of custody

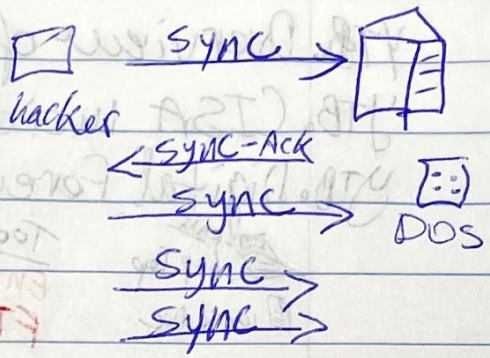
Professor Messer YTB Log Data -
security log files

Logs
- Firewalls
- Applications (Windows) Event Viewer • Syslog (Linux)
- Endpoint
  EDR/NDR/XDR
- Security Appliances
  IDS/IPS
  Proxy

William Prado
08-07-2025
Digital Forensics

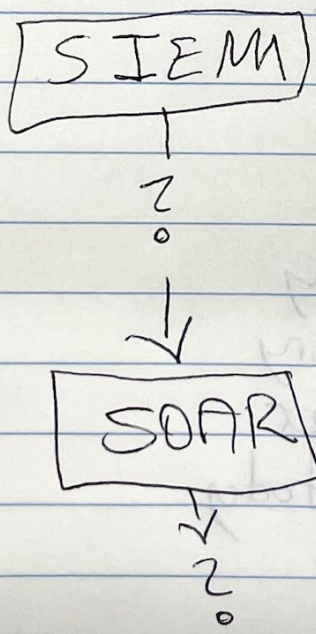
Load balancer
Cluster
Switches - span
Routers
TAP
SNMP Agent
Metadata
Data about Data

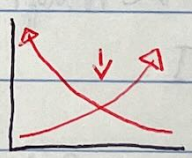
Sync Attack




geeksforgeeks.org

YTB - What is syslog?



False positives
or
False Negative

★ Critical Thinking
★ Curious

William Frodo
08/07/2025

# Incident Response
- Revention/Preparation
- Detection/Analysis
- Containment, Eradication & Recovery
- Post Incident Activity

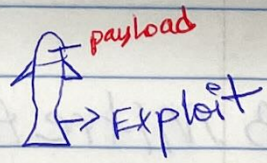
## Kill Chain Attack (Lockheed)

1) Reconnaissance
   Gathers info on target

2) Weaponize
   Exploit code + payload

3) Delivery
   Identifies vector weaponized

4) Exploit
   Weapon




5) Install
   Weapon runs remote access tool

6) C2 or C&C (Command & Control)

7) Action on Objectives
   Put into action whatever objective is.

William Prado
08/07/2025

Sunny classroom

YTB- The cyber kill chain
YTB- The cyber kill chain Explained w/ Real Examples
OSINT = open source inteligence

Mitre Attack - framework for understanding behavior Tactics & Techniques

Main components: Tactis
Techniques
Sub-Techniques
Procedures

Domains: Enterprise
mobile
Pre-attack
ICS

YTB Mitre Attack Framework

Diamond Intrusion Analysis Model

4 Parts: Adversary attacker (person/group)
Capabilities Tools (phishing email)
Infrastructure - where attack was launch (hosted)
victim - target
(person, country, host)