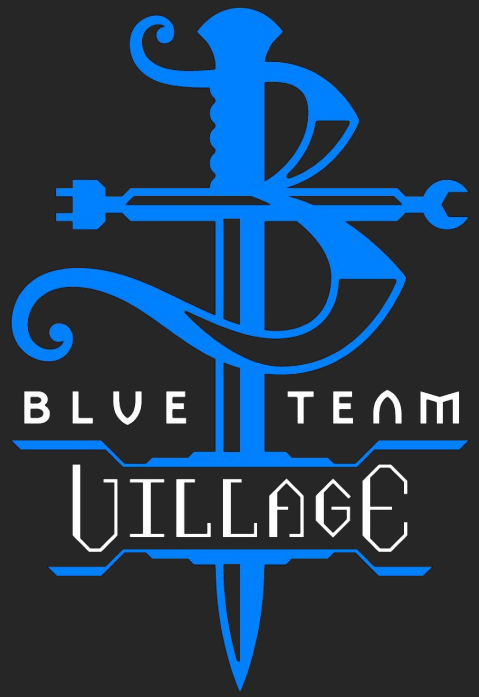
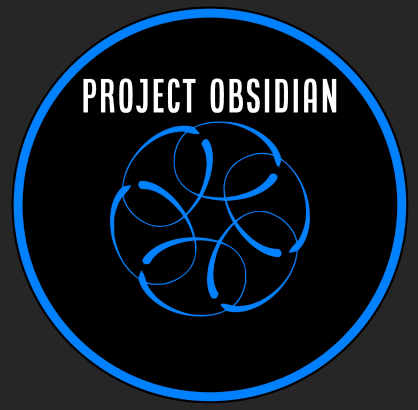
Project Obsidian



Forensics

Forensics 101

Part 2



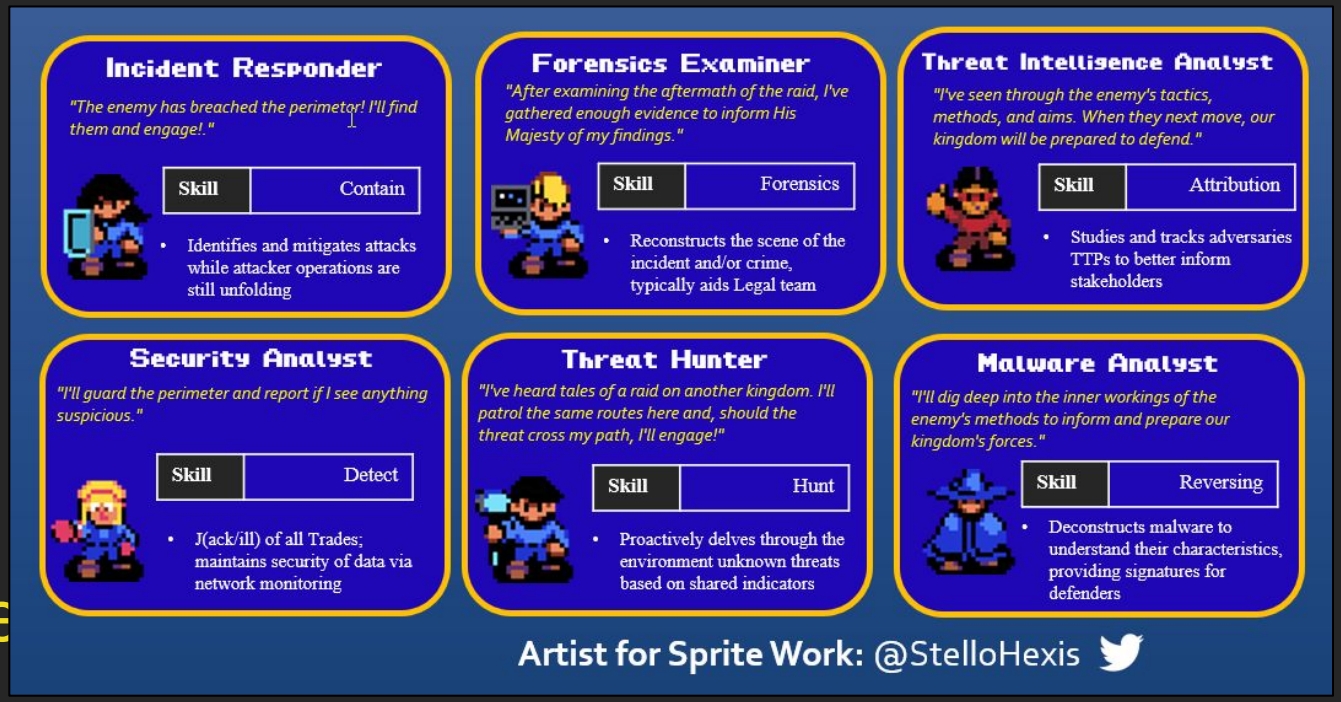
Agenda

- Supporting Digital Forensic Team
- Expectations of Digital Forensics
- Common Career Paths & Training

Supporting the Digital Forensics Team

Supporting the Digital Forensics Team

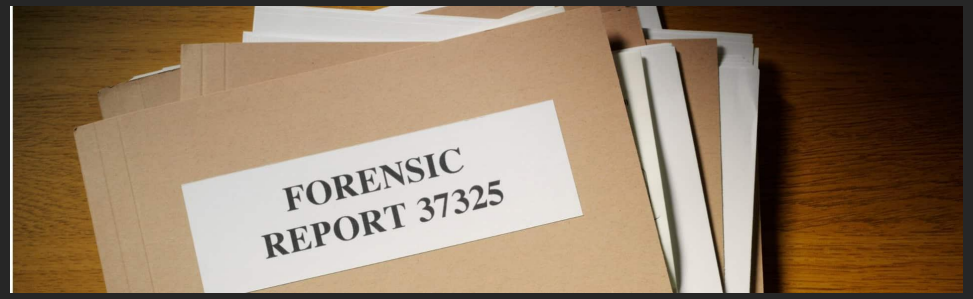
- Forensic Examiners
  - including E-discovery
- Incident Response
- Security Operations
- Malware Analysts & Reverse Engineers
- Cyber Threat Intelligence



Expectations on the Digital Forensics Team

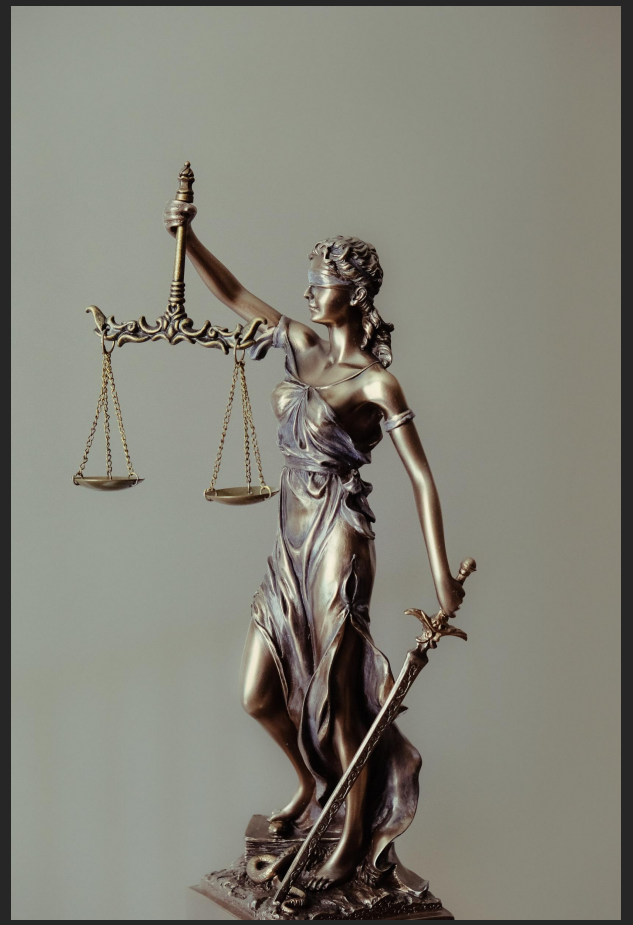
Expectations

- Reporting/Data Preparation
  - Reporting typically can be centered around one incident involving a single system, or multiple – even hundreds of systems!
  - It is up to the Digital Forensics Examiner to be able to paint a picture, and provide a narrative into what, how and why an incident occurred.



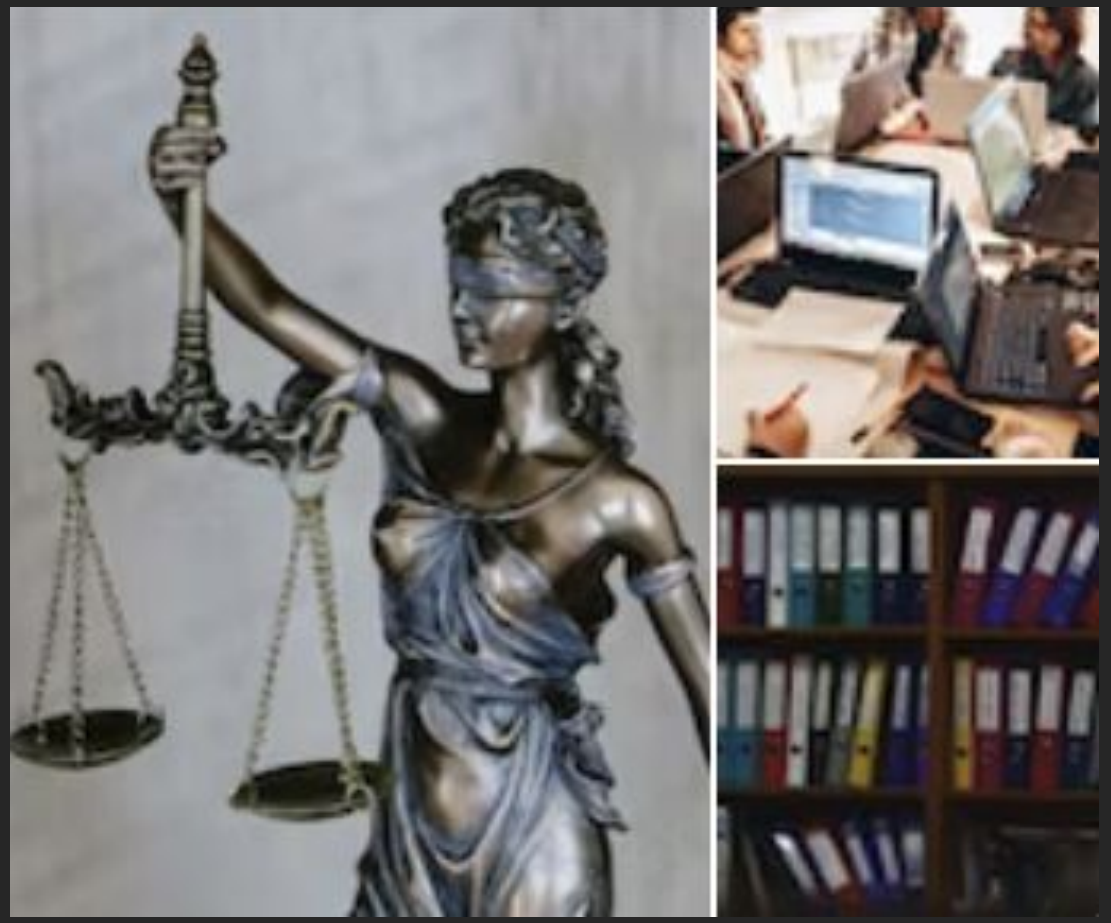
Expectations

- Court Testimonies
  - Potential to called to provide expert witness testimonies in court cases on a report, or its findings
  - Responsibilities may include
    - Organizing, and maintaining chain of custody for all evidence
    - Testing, interpreting, quantifying and communicating any findings via a presentation and/or responses to questions posed by legal counsel



Expectations

- Coordination with Legal Teams and Law Enforcement
  - Legal requirement to notify relevant law enforcement agencies upon disclosure of data breach attributed to criminal group
  - Conducting knowledge sharing (IOCs and findings) and receiving them from law enforcement to use in their ongoing digital forensics investigation.



Career Paths & Training

Common Career Paths

- Where do Digital Forensics people typically start?
  - SOC/IR, System Administrators, IT Professionals, Law Enforcement Officials
- Private Industry
  - Internal Digital Forensics, Consulting, Law Firms
- Public
  - Intelligence Agencies, Federal/State/City government units

Training Opportunities

- TryHackMe
  - Learning Paths: SOC Level 1
- Security Blue
  - Blue Team Level 1 & 2 (BTL1, BTL2)
- Antisyphon - Home of “Pay What You Can” Training
  - SOC Core Skills w/ John Strand
  - Advanced Endpoint Investigations w/ Jake Williams or Alissa Torres
- Markus Schober (Collaboration w/ TCM Security)
  - Practical Windows Forensics
- INE/eLearn Security
  - eLearnSecurity Certified Digital Forensics Professional (eCDFP)
- 13Cubed
  - Investigating Windows Endpoints
- ENISA CERT free online training materials
  - Digital forensics, Introduction to network forensics
- edX Computer Forensics online course

Training Opportunities - SANS

Host in-Depth

FOR518 - Mac and iOS Forensic Analysis and Incident Response

MacOS

FOR509 - Enterprise Cloud Forensics and Incident Response

Cloud

FOR500 – Windows Forensics Analysis

Computer (Windows)

IR & Threat Hunt-Driven

FOR608 – Enterprise-Class Incident Response & Threat Hunting

FOR508 – Advanced Incident Response, Threat Hunting, and Digital Forensics

SEC504 – Hacker Tools, Techniques, Exploits, and Incident Handling

FOR498 – Battlefield Forensics & Data Acquisition Course

Host in-Depth

Linux

FOR577 - Linux Incident Response and Threat Hunting

Mobile

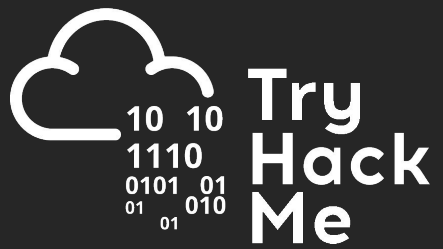
FOR585 - Smartphone Forensic Analysis In-Depth

Network

FOR578 – Advanced Network Forensics: Threat Hunting, and Incident Response

Cyber Ranges

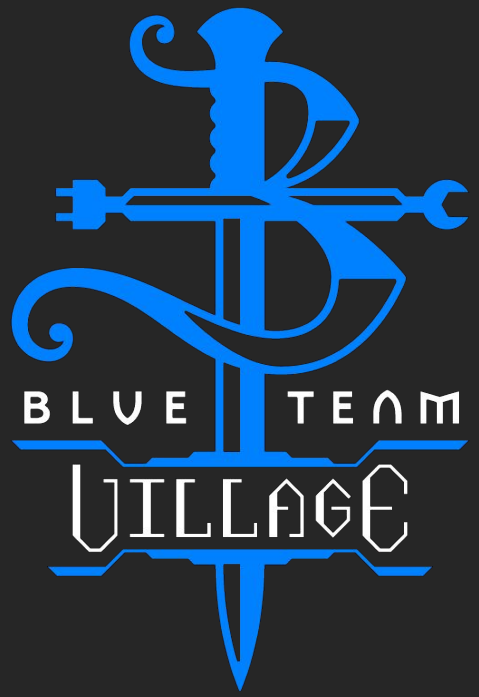
- Cyber Range – No Set-up Required
  - TryHackMe – Newbie-friendly platform from IT fundamentals to multiple disciplines
  - RangeForce – Community Edition – Offers training modules on tools such as YARA, Splunk
  - Let's Defend – Focuses on daily SOC duties to Incident Response
  - Blue Team Labs Online – Blue Team answer to HackTheBox
- Setup Necessary
  - SocVel – CTF focused on analyzing triaged data of compromised hosts
  - CyberDefenders – BlueYard – Variety of labs from old Flare-On to Boss of the SOC



References

- Antisyphon Training. https://www.antisyphontraining.com/
- B4nd1t0. 2022. Bandit's Bytes. https://banditsbytes.net/
- 2020. BlueYard - Blue Team Challenges. CyberDefenders. https://cyberdefenders.org/blueteam-ctf-challenges/
- eLearnSecurity Certified Digital Forensics Professional (eCDFP). INE. https://ine.com/learning/certifications/internal/elearnsecurity-certified-digital-forensics-professional
- Horsman, G. and Shavers, B. (2022). "Who is the digital forensic expert and what is their expertise?" WIREs Forensic Science. doi:https://doi.org/10.1002/wfs2.1453. https://wires.onlinelibrary.wiley.com/doi/full/10.1002/wfs2.1453
- 2014, November. Training for Cybersecurity Specialists. ENISA: https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material
- 2023. Investigating Windows Endpoints. 13Cubed. https://training.13cubed.com/investigating-windows-endpoints
- Pan, Y. 2017. CYBER502x - Digital Forensics. Rochester Institute of Technology (RIT). https://www.edx.org/course/computer-forensics
- Schober, M. 2022. TCM Security. https://academy.tcm-sec.com/p/practical-windows-forensics
- Tingey. 2020, May 22. Tingey Injury Law Firm. Unsplash. https://unsplash.com/@tingeyinjurylawfirm
- 2018. TryHackMe. https://tryhackme.com/
- 2022, January 20. What Is E-Discovery? Proofpoint. https://www.proofpoint.com/au/threat-reference/e-discovery
- 2022, November 7. Write a Forensic Report Step by Step. Salvation Data Technology. https://www.salvationdata.com/work-tips/write-a-forensic-report/

Thank you!



Join The Conversation
https://discord.gg/blueteamvillage

Questions?

Did you enjoy the session?
Did we miss something?
Was anything unclear or confusing?

Please Provide Feedback
feedback-obsidian@blueteamvillage.org