OSINT///ACADEMY

Course Syllabus

Instructor:	Cynthia Hetherington
Email:	Professor@hetheringtongroup.com
Office:	973-706-7525
Office Hours:	Office hours may be scheduled Monday through Saturday, please email for an appointment.
Course Delivery Method:	Online/Recorded via osintacademy.com and DSU D2L learning platform
Location & Time:	Lecture material will be released the beginning of each week to be completed by the end of each week.

COURSE DESCRIPTION

OSINT for First Responders and Transitioning Military will provide students with an overview of the fundamentals of Open Source Intelligence for industry, corporate and business needs. Students will be presented with the most effective methodologies used by cyber professionals and OSINT investigative personnel to locate and analyze information on the Internet. Students will use interactive exercises to become familiar with the volume of sensitive data on the Internet and how it can be exploited to develop highly detailed intelligence products.

REQUIRED TEXTS

- Bazzell, Michael. (2023). Open Source Intelligence Techniques: Resources for Uncovering Online Information, Tenth Edition. ISBN: 9798366360401
- Supplemental readings and other resources as assigned and supplied throughout the semester.

RECOMMENDED TEXTS

- The Manual to Online Public Records by Mike Sankey and Cynthia Hetherington.
  - https://www.vitalsource.com/products/the-manual-to-online-public-records-a-michael-l-sankey-and-cynthia-v9781889150628?
- Hetherington, Cynthia. (2015). The Guide to Online Due Diligence Investigations: The Professional Approach on How to Use Traditional and Social Media Resources. Facts on Demand Press. ISBN 1889150614
- Active Measures by Thomas Rid
- AntiFragile: Things That Gain from Disorder by Nussim Nicholas Tuleb
- Too Much Information by Cass Sunstein
- Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News by Clint Watts
- The Fifth Domain by Richard A. Clarke
- Culture Warlords by Talia Lavin

- Algorithms of Oppression: How Search Engines Reinforce Racism by Safiya Umoja Noble
- Shadow Network: Media, Money, and the Secret Hub of the Radical Right by Anne Nelson
- True or False: A CIA Analyst's Guide to Spotting Fake News, by Cindy L. Otis
- Like War: The Weaponization of Social Media
- Future Crimes by Marc Goodman
- Analysis Without Paralysis: 12 Tools to Make Better Strategic Decisions 2nd Edition by Babette E. Bensoussan and Craig S. Fleisher
- Business and Competitive Analysis: Effective Application of New and Classic Methods by Babette E. Bensoussan and Craig S. Fleisher

STUDENT LEARNING OUTCOMES

Upon completion of this course students will be able to:

- Identify and describe the goals, capabilities, and limitations associated with Open Source Intelligence
- Describe and demonstrate how to use web-based and proprietary open source search tools to conduct investigations.
- Explain and demonstrate how to conduct social media research to obtain and leverage sensitive personal data during an investigation.
- Define and explain the different types of files that contain useful metadata as well as how to access, modify and delete metadata.
- Describe and explain how to conduct reverse image searches to identify the origin, modifications, and geolocation data associated with an image or video.
- Describe and explain how to find the geolocation of an Wi-Fi access point or a subject’s IP address using Internet search tools.
- Identify and explain how to locate and leverage government documentation to verify and validate information about a subject.

COURSE OBJECTIVES

During this course students will:

- Analyze the accuracy of the publicly available data in order to validate source reliability.
- Access and analyze metadata contained within a set of provided evidence files to determine who created and modified the files.
- Investigate how much open source information can be gathered on a subject; explore the inconsistencies in the amount and types of data gathered from different sources; and examine how different sources can provide contradictory information.
- Use common search engines to locate and analyze government data to confirm or deny the validity of data located on online community sites.
- Leverage online mapping applications to locate and plot both IP addresses and WiFi Access Points

EXPECTED COURSE WORKLOAD

Students should expect a minimum of 3 hours of lecture and an additional 15 hours of labs and exercises each week for this course. Lectures are recorded and can be viewed by the student asynchronously.

REQUIRED ASSIGNMENTS (GRADED)

Requiredassignments for the course are eight quizzes, and a final examination. Students will be expected to draw on course lectures and assigned readings to complete all course assignments and Labs. *No late work will be accepted so please ensure you allot enough time to complete and turn in your work on time.*

GRADING

The final grade maximum of 1,000 Points in the course will be based upon:

Quizzes	**35%**	**See Course Schedule**
(8 Quizzes - 50 Points Each)		
Assignments		
(8 Assignments - 50 Points Each)	**35%**	**See Course Schedule**
Final Examination	**30%**	**See Course Schedule**
(Final Examination – 200 points)		

GRADING SCALE			**DISTRIBUTION**	
A	90 to 100%		900 – 1000 Points	A
B	80 to 89%		800 – 899 Points	B
C	70 to 79%		700 – 799 Points	C
D	60 to 69%		600 - 699 Points	D
E	Below 60%		0 – 599 Points	E

Week 1 - OSINT Foundations
Upon completion students will be able to examine and evaluate:

- Introduction to the Intelligence Lifecycle and C.R.A.W.L. (Communicate, Research, Analysis, Write and Listen) method
- Identify and describe the goals, capabilities, and limitations associated with open source intelligence.
  - Describe and explain the OSINT investigations.
  - Identify and describe type of investigative uses for OSINT.
- Begin to understand legal and technical boundaries.
  - Learn the CYA (Cover your Analyst) method
  - Discuss legal issues such as civil liberties
  - Threats vs. hyperbole
  - Standard US Laws
- Identify and develop web browser options.

Week 2 – OSINT Prepared
Upon completion students will be able to examine and evaluate:

- Introduction to managed attribution, and the technology models in place, and best practices for conducting OSINT safely online.
- The basics of protecting yourself while conducting online investigations
  - Computer hygiene - Virus/malware protection
- Identify and describe the capabilities and limitations associated with managed attribution.
  - Identify when managed attribution is necessary.
  - Understand the sock puppet account.
- Begin to understand legal and technical boundaries.
  - Working undercover online, misrepresentation.
  - Solutions developed by hand, and by vendors, to solve for MA on the road.
- Identify virtual machine options.

Week 3 – Search Engine Researcher
Upon completion students will be able to examine and evaluate:

- Describe and demonstrate how to use web-based and proprietary open source search tools to conduct investigations.
- Establish a working knowledge of the use of language.
  - Geo tagging
  - Global tagging
  - Keywords, buzzwords, and lingo
  - Boolean logic and the lack of logic
  - Algorithms influence on your queries.
- Identify and describe the best uses of search engines.

        - Google
        - Bing
        - Username Search tools

Week 4 – OSINT Social Media Researcher
Upon completion students will be able to examine and evaluate:

- Explain and demonstrate how to conduct social media research to obtain and leverage sensitive personal data during an investigation.
- Identify and describe the best uses of social media.
    - Deep platforms
        - Facebook
        - Twitter
        - Instagram
        - LinkedIn
        - Telegram
        - Reddit
        - Parler
        - Gab
        - 4chan
        - Other online communities
- Explain and demonstrate how to locate social data on users who do not have social media accounts, or if they have protected accounts.

Week 5 – OSINT Technical Researcher
Upon completion students will be able to examine and evaluate:

- Define and explain the different types of files that contain useful metadata as well as how to access, modify and delete metadata.
    - Images and EXIF data
    - Adobe and Microsoft metadata
- Describe and explain how to conduct reverse image searches to identify the origin, modifications, and geolocation data associated with an image or video.
    - Images, Video and EXIF data
- Describe and explain how to find the geolocation or a subject's IP address using Internet search tools.
    - Email headers and IP addresses
    - DNS database entries
    - WhoIs lookups and data interpretation
    - Traceroute
- Introduce and describe the Dark Web
    - Define the dark web
    - Perils of dark web content, and the type of content located in the dark web
    - Search tools and approaches to the dark web

Week 6 – Public Records Researcher
Upon completion students will be able to examine and evaluate:

- Identify and explain how to locate and leverage government documentation to verify and validate information about a subject.
  - Public records found online and offline.
  - The difference between countries, counties, and other global databases.
  - Vendors and aggregators versus collecting-by-hand.
- Define and explain the different types of data and database products open to the market.
  - Define PII (personal identifiable information)
  - Public record aggregators (domestic and international)
  - Industry Sources (domestic and international)

Week 7 – Analyst
Upon completion students will be able to examine and evaluate:

- Understand the needs of proper due diligence and the uses of OSINT whether mission, legal, financial, and personal matters.
  - Why money matters
  - Why we follow the money.
- Describe and explain how to conduct entity due diligence needs and expectations.
  - Comprehensive reports to Briefings
  - Budgets and turn-around-time, *aka bosses' deadline*.
- Identify the proper analytical report style to apply.
  - SWOT Analysis
  - Supply Chain and Value Chain Analysis
  - CARA Analysis
  - Due Diligence Analysis

Week 8 – Presenter
Upon completion students will be able to examine and evaluate how to collect and analyze:

- Identify and describe the different types of OSINT activity.
  - Learn to defend your work. *You are better than Google*.
  - Fact checking
    - Evidence, intelligence, and hearsay
- Document your findings.
  - Fact based information
  - Key findings and recommended next steps
  - Document your findings
- Explain how to identify, document and explain questionable information we call hearsay.

- Explain the major U.S. and International laws governing cyberspace, the restrictions they place on cyber operations, and how they can impact an organizations information gathering and reporting.

Capstone

Final Examination – Student will complete a comprehensive final examination consisting of True/False, Multiple Choice, and Short Answer questions.