OSINT - ENTRY LEVEL COURSE SYLLABUS

DAY 1

Day one begins with a general introduction regarding OSINT as an intelligence gathering discipline and it’s place within the intelligence cycle. Students are introduced to the relevant terminology and will review and analyse example cases in which OSINT had a prominent role.

As internet based OSINT investigative techniques are the main focus of this entry level course, ample time is spent on how the Internet actually works under the hood.

The penultimate topic on day one introduces the students to the plethora of both well known but also little known and special search engines. The use of (meta) search and directory engines is explained as well as the compilation of basic search strings.

The final lesson on day one is a practical exercise in which search engines will be playing a major role.

** Instructor(s) will be present in the classroom until 1 hour after the end of classes to assist with practical exercises and answer any questions. **

Learning objectives covered on day one include:

- Understanding OSINT objectives and techniques as an intelligence gathering discipline.

- Understanding what Primary Intelligence Requirements are and how these relate to OSINT investigative efforts.

- Understanding how the internet works. URL analysis, IP addressing, DNS services, the HTML scripting language, and other internet related protocols.

- Introduction to search engines and the composition of basic but effective search queries.

- Software tools and online services usable for gathering, processing, and analysis of raw data.

DAY 2

Day two begins with an evaluation of the practical exercise from day 1.

Students will make their first steps with regard to actually acquiring information from various online sources. Website investigations are the main focus of the first half of this day.

The afternoon lessons provide in-depth instruction on social media platforms and how to conduct social media investigations.

Day 2 ends with an introduction to operational security, or in other words, how to adequately prevent compromising OSINT gathering activities by adversaries.

Practical exercises will be administered throughout the day to allow students to instantly test their newly learned skills.

** Instructor(s) will be present in the classroom until 1 hour after the end of classes to assist with practical exercises and answer any questions. **

The information covered on day two includes:

- Identifying the registrant(s) of internet domain names and determining the physical location of websites.

- Understanding IP addresses, mapping domain names to IP addresses and vice versa.

- Using search engine caches and other historical archives of website content.

- Acquiring data from protected social media accounts.

- Locating and verifying social media profiles and identities.

- Search techniques and tools to target specific social media networks.

- Use of proxy servers and Web-based anonymizing tools.
DAY 3

Day three is metadata day and begins with a thorough introduction of what metadata is, and where it can be found.

Attendees then learn about how to adequately preserve both metadata- and content related data as evidence.

Instruction continues with metadata embedded in websites and e-mail messages, and how to find and acquire these, as well as alternative uses for this data.

The afternoon classes will focus on identifying and acquiring specific files like documents, photos, images, audio and movie files that are not meant to be accessible online.

The students will participate in practical exercises throughout the day.

** Instructor(s) will be present in the classroom until 1 hour after the end of classes to assist with practical exercises and answer any questions. **

The information covered on day three includes:

- Advanced search engine syntax, boolean operators, and an introduction to URL modifying.
- Analyzing metadata in websites and e-mail and determining the authenticity of acquired data through hash calculations.
- Validating OSINT related data for disseminating purposes.
- Extracting and analyzing metadata from image-, document-, audio-, and video files.
- Evaluating and classifying data retrieved through OSINT gathering techniques.
- Operational security, staying anonymous on the internet.
- Introduction to newsgroups, directory services, online databases, and how to consult expert systems.
- Disseminating OSINT products.

DAY 4

The activities on day four begin with an introduction to the dark net and online marketplaces that sell contraband or provide illegal services.

Instruction continues with a lesson on analyzing crypto currency transactions used to pay for services and products on the dark net’s online marketplaces.

Students are introduced to more advanced photo and picture tracking and tracing techniques, as well as geolocation meta data.

Instruction is provided on how to conduct due diligence through OSINT techniques, as well as addressing compliance requirements through OSINT.

The course concludes with a practical exercise in which the majority of newly acquired skills must be used in order to meet the Primary Intelligence Requirements.

** Instructor(s) will be present in the classroom until 1 hour after the end of classes to assist with practical exercises and answer any questions. **

The information covered on day four includes:

- Image and photo tracking, tracing, and analysis.
- Crypto currency transactions and block chain analysis.
- Determining historic ownership of Bit Coins.
- Introduction to geolocation and photo geolocation.
- Conducting due diligence and compliance through OSINT.
- Practical exam. After successful completion the OSINT entry level certificate is issued.