Agenda

(last changed 25.10.2017)

The content of the various sessions may slightly change until the event. Whenever changes occur, we will update this page accordingly.

For the hands-on sessions and tutorials please bring a full notebook (not a tablet, such as IPad), preferably MS Windows, which you can connect to a public Wi-Fi.
It is also possible to share a computer between two users in case you are attending the course with colleagues from your organisation.

Tuesday, 28.11.2017

Arrival and transfer to the hotel.

Wednesday, 29.11.2017

Time			
09:30- 09:40	Welcome Day 1 & Overview *DG Joint Research Centre*		
09:40 - 10:30	International co-operation in Financial Criminal Investigations ████████, *Dutch Tax Authorities* (abstract below)		
10:30 - 10:45	*Coffee Break*		
10:45 - 11:45	SIRIUS as a law enforcement framework for internet investigations ████████, *EUROPOL* (abstract below)		
11:45 - 12:15	Social Media Monitoring for Awareness of Security Threats against VIPs: opportunities and challenges ████████, *DG HR, European Commission* (abstract below)		
12:15 - 12:30	Quick overview of the courses and tutorials *Text and Data Mining Unit, DG Joint Research Centre*		
12:30 - 14:15	*Lunch Break*		
14:30 - 16:00	On-line news monitoring with Europe Media Monitor (EMM) (description below)	EMM OSINT Suite Introduction (description below)	Core Tools for Assembling Information Extraction Pipelines (description below)
16:00 - 16:15	*Coffee Break*		
16:15 - 17:30	On-line news monitoring with Europe Media Monitor (EMM)	EMM OSINT Suite Introduction	Core Tools for Assembling Information Extraction Pipeliness

Thursday, 30.11.2017

Time			
09:30	Welcome Day 2		

09:30 - 10:30	Computer support for analyzing violent extremism in online environments		
	, *Swedish Defence Research Agency*		
	(abstract below)		
10:30 - 10:45	*Coffee Break*		
10:45 - 12:30	On-line news monitoring with Europe Media Monitor (EMM)	EMM OSINT Suite Introduction	Core Tools for Assembling Information Extraction Pipeliness
12:30 - 14:15	*Lunch Break*		
14:30 - 16:00	On-line news monitoring with Europe Media Monitor (EMM)	EMM OSINT Suite Introduction	Core Tools for Assembling Information Extraction Pipeliness
16:00 - 16:15	*Coffee Break*		
16:15 - 17:30	On-line news monitoring with Europe Media Monitor (EMM)	EMM OSINT Suite Introduction	Core Tools for Assembling Information Extraction Pipeliness
20:00 - 22:30	Social Dinner		

Friday, 01.12.2017

Time	Session		
09:30	Welcome Day 3		
09:30 - 10:00	Use of Open-Source Information in the IAEA Safeguards Department *Christopher Eldridge, International Atomic Energy Agency* (abstract below)		
10:00 - 10:30	JRC Presentation on the latest OSINT-related developments and activities Text and Data Mining Unit, DG Joint Research Centre		
10:30 - 10:45	*Coffee Break*		
10:45- 12:15	On-line news monitoring with Europe Media Monitor (EMM)	EMM OSINT Suite Introduction	Core Tools for Assembling Information Extraction Pipeliness
12:15 - 12:30	Wrap-Up & Feedback		
12:30 - 14:00	*Lunch*		
14:15	*Bus transfer to airports*		

Expert Presentations Abstracts

International co-operation in Financial Criminal Investigations

Presenter: (Dutch Tax Authorities)

Abstract:

Technological developments make things poss ble that we could not have imagined twenty-five years ago. Forms of communication, producing things, transporting goods, the way in which transactions take place are changing constantly, not only in legal, but also in illegal

businesses. To effectively fight serious financial cross border criminality, international cooperation is a necessity.

The past year two international initiatives were launched which had financial criminal investigations as a the starting point. ENFIN, a European knowledge Network were members and partners can exchange experiences, methods and new developments on Financial Investigations, and FCInet a virtual solution that makes data matching and exchange easy and enlarge the international co-operation possibilities. FCInet is based on the proven technology and is supported by the Forum of Tax Crime Investigations (FHTCI) of the OECD. Both networks consists of Law Enforcement organisations specialised in financial investigations and Tax and Customs administrations. They collaborate with respect to the differences in working methods, (privacy) legislation, data protection and independence of the participating organisations. The presentation will contain backgrounds on the ENFIN and FCInet, the aims, partners, steps taken and the outlook for 2018.

SIRIUS as a law enforcement framework for internet investigations

Presenter: [REDACTED] (EUROPOL)

Abstract:

Nowadays, investigators working on a case cannot avoid investigating the digital footprintof those who plan terrorist attacks or are suspected of recruitment, training and financing of terrorism, as well as incitement to commit a terrorist offense, including relationships, communication means, financial aspects, logistics, centres of interest and behavioural activity.

Whilst these information sets were historically under the remit of national entities, they have now acquired a global perspective and are owned by Online Service Providers, oftentimes based outside of the EU territory. Further complexity stems both from the volatility of data held across different legislations, as well as its volume and the urgency with which this information is needed in the context of a CT case In the attempt to cope with these challenges and to maximize the level and the quality of operational support provided, we have recently launched SIRIUS, a project which aims to cater for the investigators' needs in an online environment. Available only to law enforcement authorities and deployed in a closed and secured environment, SIRIUS is the place where all the information related to Online Service Providers, and how to increase the investigation efficiency can be found, with manuals, tips, forums, Q&A, etc. Additionally, the platform will also include a repository for the collaborative development of tools to support investigations of crimes facilitated by the Internet, developed by and intended for the Law Enforcement community.

Social Media Monitoring for Awareness of Security Threats against VIPs: opportunities and challenges

Presenter: [REDACTED] (DG HR, European Commission)

Abstract:

Identifying poss ble adversaries is a key element of Security Threat Assessments. When assessing threats against persons with high public visibility, monitoring Social Media may seem a promising idea in order to identify potential groups, persons, ideologies developing a specific hate narrative. Indeed, social media features all sort of opinion trends and are often used as an echo chamber for propaganda purposes. They can thus be seen as an easily accessible and abundant source for Personal Threat Assessment purposes. However, exploitation of Social Media material into actionable intelligence (e.g. to support decisions on the set up of VIP security measures) poses several methodological and technical challenges. The purpose of this presentation is to stimulate discussion on such challenges, rather than descr bing pre-cooked solutions.

Computer support for analyzing violent extremism in online environments

Presenter: [REDACTED] (FOI – Swedish Defence Research Agency, Sweden)

Abstract:

This talk gives an overview over the research done at the Swedish Defense Research Agency (FOI) on developing and applying tools for analyzing violent extremism in online environments. The talk focuses on analysis of text data, and presents some of the core technologies we use to deal with large-scale and noisy data. We also provide examples from two recent studies where we have applied our tools to large collections of propaganda material from IS, and to large collections of web data from Swedish right-wing extremist groups.

Use of Open-Source Information in the IAEA Safeguards Department

Presenter: [REDACTED] (IAEA - International Atomic Energy Agency)

Abstract:

The IAEA Department of Safeguards makes extensive use of open-source information in support of its mission to verify the compliance of Member States with their safeguards obligations. Open-source information is one of several data streams that facilitate the on-going State evaluation process. This presentation will review the department's work with open-source information, which includes both routine monitoring of news and other information sources and targeted searching, to support verification activities both in headquarters and in the field. Sources used include websites, newsfeeds, scientific and technical literature, and databases containing information on imports and exports of commodities. The on-going, productive relationship between the IAEA and JRC Ispra has significantly strengthened the Department of Safeguards' capabilities in routine monitoring of open sources, and the IAEA is now exploring the possibility of using the EMM OSINT Suite to streamline and improve the department's capability to perform targeted searches of open sources for information of safeguards relevance.

Courses and Tutorials

On-line news monitoring with Europe Media Monitor (EMM)

Overview:

This course provides a general overview of EMM technology and related tools. It shows with practical examples how Text Mining and Analysis (TMA) can effectively support the daily work of analysts. The platform processes every day about 300,000 news articles providing: language detection, categorization, language recognition, entity extraction, quote extraction, geotagging, tonality, duplicate detection, categorisation, indexing and searching, clustering, statistics and event extraction. Dedicated Graphical User Interfaces allow analysts to display and browse all metadata and create reports and/or newsletters.

The course structure includes hands-on sessions based on a common use case: participant will learn how to configure the platform in order to capture news related to their topics of interest, browse the results, produce newsletters and send notifications.

This course is targeting people who has just started using EMM or who need to assess whether to adopt it as media monitoring platform.

Requirements:

Some prior experience with on-line media monitoring or information extraction tools of any kind is an advantage. The participants should bring with them a notebook with an Internet browser (IE, Firefox, Chrome, etc.).

EMM OSINT Suite

Overview:

The EMM Open Source Intelligence Suite is a desktop software application which helps to find, acquire and analyse data from the Internet and local sources. It provides automatic means to gather intelligence from open available sources by removing the need to search manually through vast data sets. EMM OSINT Suite comprises a set of tools to support the main processes of intelligence gathering from open sources.

The course gives an introduction into basic and advanced features of the software, such as acquisition of documents, text extraction and analysis.

Requirements:

The participants should bring with them a notebook (preferably MS Windows based). Some prior knowledge of basic internet research techniques is a plus.

Core Tools for Assembling Information Extraction Pipelines

Overview:

This course provides a hands-on overview of core text processing modules developed by JRC that can be exploited to assemble dedicated Information Extraction processing chains. In particular, tools for tokenisation, sentence splitting, morphological analysis, large-size dictionary look up and annotation, simple and complex pattern matching will be presented. The participants will learn how to configure and combine these tools in order to build integrated solutions for the extraction of various types of structures, ranging from simple date expressions, bank identifiers, to relations that hold between entities found in text, .e.g., "PERSON met with PERSON" or "PERSON works for ORGANIZATION". The aspects on how the developed solutions can be integrated in other frameworks-workflows using the API (Application Programming Interface) will also be covered.

This course is particularly thought for people who want to gain deeper insight on how to develop Information Extraction tools and related resources on their own, and thus, have a more control over the underlying processes.

Requirements:

Some prior experience with using Information Extraction tools of any kind is required (e.g., EMM OSINT Suite). Knowledge of Java programming language is not essential, but will be highly advantageous in the context of the more advanced topics covered. The participants should bring with them a notebook with Java Virtual Machine installed on it (version 1.7 at least).