DRAFT BASIC LEVEL TRAINING PROGRAMME

Location: Bucharest, Romania

Venue: DIICOT headquarters (24 Calea Griviței, District 1)

Language: English (B2 level needed)

Session 1 # 18-21 September 2017

Session 2 # 06-09 November 2017

Session 3 # 20-23 November 2017

DAY 1 / MONDAY	**TRAINING TOPICS**
09.00-10.30	**Legal English** Cybercrime specific terminology
10.30-11.00	**Coffee break**
11.00-13.00	**HOW THE INTERNET WORKS** - How websites work - VPN, Proxy servers - IPv4, IPv6, servers, etc. - Internet environment What an investigator should know about it?
13.00-14.30	**Lunch break**
14.30-17.00	**COMMUNICATION PLATFORMS** - Social media, metadata found in social media - Encryption, Jabber, PGP - Chat programs, Instant messaging **Practical exercises:** How to arrange a VPN? How a peer to peer network works?
DAY 2/ TUESDAY	
09.00-10.30	**Legal English** Cybercrime specific terminology
10.30-11.00	**Coffee break**
11.00-13.00	**PRINCIPLES**

	- Definition of undercover agents and informants - Legal conditions/requirements - Type of activities - Entrapment, ethics and human rights approach - Legal hacking - Limits of gathering information, gathering information in online investigations - Documenting online evidence - How do we search for information (restricted/ non-restricted sources) - Typology of crime with online aspects - Cooperation with other institutions/private sector - International approach -MLA, JITs, - How to authorize an international undercover online operation **COUNTRY SPECIFICS** ***10 minutes presentations for each of the 6 countries (RO, BG, IT and 3 other EU MS); each presentation should be delivered by one delegate for each country***
13.00-14.30	**Lunch break**
14.30-17.00	**INVESTIGATOR'S PROFILE** - The undercover agent, the handler - Recruiting and training of online undercover agents - Recruiting and use of informants - Damage assessment, Exposure, Protection. - Profile and training of an undercover investigator on Internet: skills, costs, recruiting informants - Content of an undercover operation (controlled delivery of ex-filtered personal data, hosting networks, freelancing, vetting, levelling) - Debriefing - Short time vs long time ops - Distinction between different types of activities - Crime as a service
DAY 3/ WEDNESDAY	
09.00-10.30	**Legal English**

	Cybercrime specific terminology
10.30-11.00	**Coffee break**
11.00-13.00	**PREPARATION** **1. ANONYMITY** - Preparing the system - Anonymizing services - Software Practical exercises
13.00-14.30	**Lunch break**
	PREPARATION **2. OPEN SOURCE INVESTIGATIONS** - OSINT - Automated solutions - Practical exercises **3. DARK WEB/ DEEP WEB INVESTIGATIONS** - TOR, markets, forums - Challenges in the development of an undercover profile - Crypto-currencies
DAY 4/ THURSDAY	
09.00-10.30	**Legal English** Cybercrime specific terminology
10.30-11.00	**Coffee break**
	EXTRACTION AND EXPLOITATION OF INFORMATION/ EVIDENCE - Evidence and means of evidence - Online searches - Evidence, reports, material evidence, take down
13.00-14.30	**Lunch break**
14.30-17.00	Case studies Practical exercises Feedback and conclusions