



# CERT participation in incident handling related to the Article 13a obligations

Handbook, Document for teachers

September 2014



\*\*\*\* \* enisa

European Union Agency for Network and Information Security



# About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at <u>www.enisa.europa.eu</u>.

# Acknowledgements

#### **Contributors to this report**

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

#### **Agreements or Acknowledgements**

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

# Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.



#### Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

#### **Copyright Notice**

© European Union Agency for Network and Information Security (ENISA), 2013

Reproduction is authorised provided the source is acknowledged.



# **Table of Contents**

1	Introduction	1
2	General Description	1
3	EXERCISE COURSE	2
3.1	Introduction to the exercise	2
3.2	Task 1: Building a technical environment for analysing network monitoring data	4
3.3	Task 2: Analysing of network monitoring data	5
3.4	Task 3: Evaluating countermeasures values	14
4	Summary of the exercise	16



# **1** Introduction

### Goal

This exercise provides students with information about rules, procedures and best practice in handling incident related to obligation for internet service providers described in the Article 13a of the European Telecom Package.<sup>1</sup>

#### **Target audience**

Incident handlers and CERT managers responsible for incident handling procedures within an organisation

#### **Course Duration**

3 hours

#### Frequency

Once for each new CERT member

# Structure of this document

Task	Duration
Introduction to the exercise	10 min
<i>Task 1:</i> Building technical environment for analysing network monitoring data	30 min
Task 2: Analysing of network monitoring data	90 min
<i>Task 3:</i> Preparing report according to the Article 13a template report	30 min

# 2 General Description

The purpose of this exercise is to prepare participants to be ready to analyse a set of data related to a DDoS attack. The proposed type of attack is similar to those that should be reported to the Regulatory Authority according to the rules and obligations for internet service providers (ISPs) described in Article 13a of the European Telecom Package. In this particular example, the attack is against an important online service provided by ISP and used by ISP customers for e-services. The service for customers is not available due to on-going DDoS attack. Additionally due to the DDoS attack, the network service is temporarily unavailable.

<sup>&</sup>lt;sup>1</sup> Directive 2009/140/ec of the European Parliament and of the Council (dealing with electronic communications) - <u>http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF</u>



During the exercise participants will learn:

- how to analyse network traffic data related to the attack;
- what kind of information can be obtained from network traffic data;
- how to prepare the report that should be used for reporting security incidents according to Article 13a.

# **3** EXERCISE COURSE

The course of this exercise is as follows. All assumptions and discussions should be moderated by the trainer.

# **3.1** Introduction to the exercise

At the beginning of the exercise you should introduce participants to the attack that occurred in the network of the ISP. Participants play the role of representatives of the ISP CERT team, which is responsible, along with other duties, for analysing network monitoring data and preparing an incident security report for the national regulatory authority.

There are three different levels of incident notifications and obligations related to them:<sup>2</sup>

- a service provider reporting to the national regulatory authority;
- a national regulatory authority reporting to other national regulatory authorities;
- a national regulatory authority reporting to ENISA.



These obligations are described in paragraph 3 of Article 13a<sup>3</sup>:

ENISA

and EC

Figure1: Reporting schemes of Article 13a<sup>2</sup>

Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.

NRA B

In practice it means that the provider (mainly this will relate to ISPs) should continuously monitor the level of the security of their telecommunication resources. Detection and especially reaction and handling to observed incidents should be based on the best practices related to incident handling activities,<sup>4</sup> which means that incident handling capability should exists in all providers.

A citation from Article 13a of the European Telecom Package: "Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and the European Network and Information Security Agency (ENISA). The national regulatory

<sup>&</sup>lt;sup>2</sup> 'Technical Guideline on Reporting Incidents – Article 13a Implementation' - <u>http://www.enisa.europa.eu/activities/Resilience-and-</u>

<sup>&</sup>lt;u>CIIP/Incidents%20reporting/Technical%20Guidelines%20on%20Incident%20Reporting/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting</u>

<sup>&</sup>lt;sup>3</sup> http://ec.europa.eu/information\_society/policy/ecomm/doc/library/regframeforec\_dec2009.pdf

<sup>&</sup>lt;sup>4</sup> ENISA Good Practice Guide for Incident Management: <u>http://www.enisa.europa.eu/activities/cert/support/incident-</u> <u>management</u>



authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest."

In particular cases, where the security incident could have a significant influence on the level of security in countries other than the country of the incident's origin, cooperation and effective communication between national regulatory authorities is very important. Thanks to this cooperation an appropriate warning and alerting in other countries is possible. It is worth adding that this internal country warning and alerting activities are very often based on CERT involvement in these processes.

A citation from Article 13a of the European Telecom Package: "Once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph."

The purpose of such reporting is to gather relevant information about Internet network breaches. The assumption is that it will help authorities to better understand new trends and mechanisms in Internet threats as well as being an important element in raising the public's level of awareness regarding Internet security.

In this exercise a security incident related to the ISP network is discovered: the online service for customers is not available due to on-going DDoS attack. Additionally due to the DDos the network service is temporarily unavailable. There is no clear information on how long it could last, what requests might come from customers in case they have no access to their data or network.

# **3.2** Task 1: Building a technical environment for analysing network monitoring data

Participants will have to build a technical environment for analysing network monitoring data. They will need to install Wireshark software<sup>5</sup> for extracting data from Pcap files (packet capture).

Additionally as a recommended tool they would need the tcpdump application. Alternatively the technical environment can be prepared by trainer.

The Wireshark application installation guide can be found in *Wireshark User's Guide* in Chapter 2: 'Building and Installing Wireshark'.<sup>6</sup>

<sup>&</sup>lt;sup>5</sup> <u>http://www.wireshark.org</u>

<sup>&</sup>lt;sup>6</sup> <u>http://www.wireshark.org/download/docs/user-guide-a4.pdf</u>



8 8 9 9 6	🗑 📔 🖾 🗶 C	🚊   Q 🔶 🤿 '	<b>)</b> 7 1	L   🗐 📑   c = () 📅   🕁 🖹 💽 💥   📀
Filter:		▼ Expres	sion Clea	ar Apply
No. Time	Source	Destination	Protocol	Length Info
1 0.00000000	10.157.5.204	192.168.0.1	TCP	54 13083 > http [ACK] Seq=1 Ack=1 Win=64511 Len=0
2 0.000005000	192.168.0.1	10.157.5.204	HTTP	2102 Continuation or non-HTTP traffic[Packet size limited during capture]
3 0.003981000	10.230.46.182	192.168.0.1	ТСР	66 46921 > http [ACK] Seq=1 Ack=1 Win=6432 Len=0 TSval=970311826 TSecr=8857
4 0.004149000	192.168.0.1	10.14.148.186	HTTP	269 Continuation or non-HTTP traffic[Packet size limited during capture]
5 0.004761000	99.29.79.36	192.168.0.1	ICMP	70 Destination unreachable (Communication administratively filtered)
6 0.005275000	10.157.5.204	192.168.0.1	ТСР	54 13083 > http [ACK] Seq=1 Ack=1025 Win=65535 Len=0
7 0.005980000	200.150.68.218	192.168.0.1	UDP	256 Source port: chargen Destination port: distinct
8 0.007547000	203.218.45.124	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
9 0.008059000	99.29.79.36	192.168.0.1	ICMP	70 Destination unreachable (Communication administratively filtered)
10 0.009933000	10.157.5.204	192.168.0.1	ТСР	54 13083 > http [ACK] Seq=1 Ack=2049 Win=64511 Len=0
11 0.009978000	192.168.0.1	10.157.5.204	HTTP	2102 Continuation or non-HTTP traffic[Packet size limited during capture]
12 0.010950000	99.150.164.202	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
13 0.011158000	200.196.50.249	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct
14 0.011883000	200.196.50.249	192.168.0.1	IPv4	1049 Fragmented IP protocol (proto=UDP 0x11, off=5920, ID=260f)
15 0.011993000	200.137.128.25	192.168.0.1	IPv4	297 Fragmented IP protocol (proto=UDP 0x11, off=1480, ID=2684)
16 0 012111000	200 137 128 25	102 168 0 1	HINP	1514 Source nort: chargen Destination nort: distinct
▶ Frame 409: 1514 by	tes on wire (12112 bit	ts), 96 bytes captured	(768 bits	)
▶ Ethernet II, Src:	JuniperN_a5:0e:80 (50	c5:8d:a5:0e:80), Dst:	SuperMic_	35:81:68 (00:25:90:35:81:68)
▶ Internet Protocol	Version 4, Src: 200.14	45.25.26 (200.145.25.2	6), Dst: 1	92.168.0.1 (192.168.0.1)
▶ User Datagram Prot	ocol, Src Port: charge	en (19), Dst Port: dis	tinct (999	9)
▶ Data (54 bytes)				
0000 00 25 90 35 81	1 68 50 c5 8d a5 0e 8	0 08 00 45 00 .%.5.h	ηΡE	
0010 05 dc 1b 5c 20	0 00 6d 11 6a 60 c8 9	1 19 1a cO a8\ .	.m. j`	
0020 00 01 00 13 27	7 Of 15 1d 6d 74 20 2	1 22 23 24 25'.	mt !"#\$	%
0030 26 27 28 29 28	a zu zc za ze zr 30 3	1 32 33 34 35 &'()*4	+,/01234	-
File: "/home/user/Democration of the second seco	ownloads/dat Packets	: 5809634 Displayed: 5809	634 Marked	: 0 Load time: 1:10.129 Profile: Default

Figure 2: Using Wireshark

The figure presents the Wireshark interface with pcap loaded into the application; information about packets can be seen in the picture.

# **3.3 Task 2: Analysing of network monitoring data**

Network monitoring data, provided to participants in this exercise, includes different types of network TCP/IP protocol data, like ICMP flows and UDP flows. Participants should make the following types of analysis.

#### Subtask 1 – determination of time and volume of the attack

Firstly, participants should create a short summary including basic information of each pcap file they have. They should check:

- the start and end time of capture;
- the size of captured packets;
- the total number of packets as well as average packet/byte rates;

This information should give a general overview of the size of data that are going to be analysed and allow the placement of PCAP files on the timeline (note that capture times of separate PCAPs can overlap).

All of this information can be easily checked using the capinfos tool that comes with Wireshark:<sup>7</sup>

<sup>&</sup>lt;sup>7</sup> http://www.wireshark.org/docs/man-pages/capinfos.html



\$ capinfos /path/to/pcap/file.pcap

<pre>@debian1:~/ddos</pre>	\$ capinfos ddos.pcap
File name:	ddos.pcap
File type:	Wireshark/tcpdump/ libpcap
File encapsulation:	Ethernet
Packet size limit:	file hdr: 96 bytes
Packet size limit:	inferred: 96 bytes
Number of packets:	5809766
File size:	631017266 bytes
Data size:	6412591020 bytes
Capture duration:	484 seconds
Start time:	2012
End time:	2012
Data byte rate:	13242515.58 bytes/sec
Data bit rate:	105940124.63 bits/sec
Average packet size:	1103.76 bytes
Average packet rate:	11997.63 packets/sec
SHA1:	f97f61a03813c289d685749d7dafd3c3f1e56fbd
RIPEMD160:	e010c9cceaaac66188eceefa761044d5db254750
MD5:	00e4502241fc357415218cf4ce32bba1
Strict time order:	False
@debian1:~/ddos	\$

Figure 3: Using capinfos

Figure 3 shows the output of the capinfos application, allowing the user to obtain general information about the pcap file. Information consists of file size, number of captured packets, checksums, capture times and also a few average values.

In the next step, participants should examine the captured traffic and try to determine what kind of DDoS attack was performed. Usually, during a DDoS attack, more than one DDoS technique is used; or there are separate and distinct attack sources. At this point, they should try to create a Wireshark filter <sup>8</sup> or a tcpdump Berkeley Packet Filter (BPF) filter,<sup>9</sup> which would allow filtering out each type of DDoS attack stream.

In fact there were two kinds of attacks and this should be found out by participants (see below).

- ICMP flood
- UDP flood

In the ICMP flood, all ICMP packets were type 3 (Destination Unreachable) with codes 3 (Destination Port Unreachable) and a few cases of code 1 (Destination host unreachable) and 13 (Communication administratively prohibited).

<sup>&</sup>lt;sup>8</sup> More on Wireshark filters: https://www.wireshark.org/docs/dfref/

<sup>&</sup>lt;sup>9</sup> More on tcpdump filters: http://www.cs.ucr.edu/~marios/ethereal-tcpdump.pdf



Iter: icmp D. Time 1501 0.941522000 1589 0.961686000 1592 0.965316000	Source	Destination	pression Clear	Apply			
o. Time 1501 0.941322000 1589 0.961686000 1592 0.965 <u>316000</u>	Source	Dectiontion					
1589 0.961686000 1592 0.965 <u>3</u> 16000	203.210.43.124	Descination	Protocol Ler	ngth Info	NADIE (FULL UNLEACHAD	18)	
1592 0.965316000	99.29.79.36	192.168.0.1	ICMP	70 Destination unread	hable (Communication	administratively fi	ltered)
1596 0.967381000	99.150.164.202 99.156.206.232	192.168.0.1	ICMP	74 Destination unread	hable (Port unreachab hable (Port unreachab	le)	
1608 0.974086000	203.218.45.124	192.168.0.1	ICMP	74 Destination unread	hable (Port unreachab	le)	
1617 0.979676000	192.168.0.1	200.196.50.249	ICMP	590 Destination unreach	hable (Port unreachab	le)	
1622 0.981248000	99.29.79.36	192.168.0.1	ICMP	70 Destination unread	hable (Communication	administratively fi	ltered)
1631 0.987270000	99.156.206.232	192.168.0.1	ICMP	74 Destination unreach	hable (Port unreachab	le)	
1640 0.995175000 1645 0.997974000	203.218.45.124 99.150.164.202	192.168.0.1	ICMP ICMP	74 Destination unreact 74 Destination unreact	hable (Port unreachab hable (Port unreachab	le) le)	
1667 1.010158000	99.150.164.202	192.168.0.1	ICMP	74 Destination unreac	hable (Port unreachab	le)	
1675 1.013983000 1689 1.022240000	99.156.206.232 203.218.45.124	192.168.0.1 192.168.0.1	ICMP ICMP	74 Destination unreact 74 Destination unreact	hable (Port unreachab hable (Port unreachab	le) le)	
1693 1.022834000	99.29.79.36	192.168.0.1	ICMP	70 Destination unreac	hable (Communication	administratively fi	ltered)
internet II, Src: - (internet Protocol M Internet Control M Type: 3 (Destinat Code: 3 (Port unr Checksum: 0x17e4	<pre>value (392 bit luniperN_a5:11:c0 ( /ersion 4, Src: 99. issage Protocol ion unreachable) eachable) [incorrect, should Version 4, Src: 15</pre>	be 0xb447]	Dst: SuperMic_35 164.202), Dst: 19	.81:68 (00:25:90:35:81: 92.168.0.1 (192.168.0.1 .164.202 (99.150.164.20	68) ) )22)		
User Datagram Pro Data (3 bytes)	tocol, Src Port: di	LSTINCT (9999), DST P	ort: chargen (19	)			
00 00 25 90 35 81 10 00 3c 20 b3 00 20 00 01 03 03 17	68 50 c5 8d a5 11 00 74 01 5d 04 63 e4 00 00 00 00 45	c0 08 00 45 00 .% 96 a4 ca c0 a8 .< 5 00 00 20 b0 51	5.5.hPE. t. ].c Q				
00 00 25 90 35 81 10 00 3c 20 b3 00 20 00 01 03 03 17 30 00 00 f3 11 4e File: "/home/user/Do gure4: ICMP	68 50 c5 8d a5 11 00 74 01 5d 04 63 e4 00 00 00 04 57 71 c0 a8 00 01 63 wnloads/dat Pack packet of t	c0       08       00       45       00          96       a4       ca       c0       a8          90       00       02       b0       51          96       a4       ca       27       0f          ets:       5809634 Displayed:       ype       3       (Destination)	5.5.hPE. 	oad time: 1:01.707 chable) with co	de 3 (Destinat	E Profile: Default	reachable
00 00 25 90 35 81 10 00 3c 20 b3 00 20 00 01 03 03 17 30 00 00 f3 11 4e File: "/home/user/Do gure4: ICMP	68 50 c5 8d a5 11 00 74 01 5d 04 63 e4 00 00 00 04 63 71 c0 a8 00 01 63 wnloads/dat Pack packet of tr	c0 08 00 45 00       .*         3 96 a4 ca c0 a8       .<         5 00 00 20 b0 51          3 96 a4 ca 27 0f          ets: 5809634 Displayed:         ype       3         (Destination)         (Destination)	.5.hPE.     .eq.     .Nqc'. 197190 Marked: 0 L ation Unrea	oad time: 1:01.707 chable) with co	de 3 (Destinat	Profile: Default	reachable
00 00 25 90 35 81 10 00 3c 20 b3 00 20 00 01 03 03 17 30 00 00 f3 11 4e File: "/home/user/bo gure4: ICMP Iter: icmp	68 50 c5 8d a5 11 00 74 01 5d 04 63 e4 00 00 00 04 63 71 c0 a8 00 01 63 wwnloads/dat Pack packet of ty	C 0 08 00 45 00     S 96 a4 ca c0 a8     S 96 a4 ca 27 0f     S 96 a4 ca 27 0f     tets: 5809634 Displayed:     ype 3 (Destination		oad time: 1:01.707 <b>chable) with co</b> Apply apth lafe	de 3 (Destinat	E Profile: Default tion Port Uni	reachable
00 00 25 90 35 81 10 00 3c 20 b3 00 20 00 01 03 03 17 30 00 00 f3 11 4e File: "/home/user/Do gure4: ICMP Iter: icmp b. Time	68 50 c5 8d a5 11 00 74 01 5d 04 63 e4 00 00 00 04 63 e71 c0 a8 00 01 63 wnloads/dat Pack packet of tr Source	C 08 00 45 00     S 96 a4 ca c0 a8     S 96 a4 ca 27 0f     S 96 a4 ca 27 0f     tets: 5809634 Displayed:     ype 3 (Destination		oad time: 1:01.707 <b>chable) with co</b> Apply ngth Info 74 Destingtion unread	de 3 (Destinat	Profile: Default tion Port Uni	eachable
00 00 25 90 35 81 00 03 c2 0b 3 00 20 00 01 03 03 17 30 00 00 f3 11 4e File: "/home/user/Do gure4: ICMP Iter: icmp b. Time 2372 1.359855000 2380 1.364910000	68 50 c5 8d a5 11 00 74 01 5d 04 63 71 c0 a8 00 01 63 wnloads/dat ≥ Pack packet of to Source 203.218.45.124 99.156.206.232	C 0 08 00 45 00     S 96 a4 ca c0 a8     S 96 a4 ca 27 0f     S 96 a4 ca 27 0f     ype 3 (Destination		oad time: 1:01.707 <b>chable) with co</b> Apply ngth Info 74 Destination unreac 74 Destination unreac	de 3 (Destinat	Profile: Default tion Port Uni	reachable
00 00 25 90 35 81 0 00 3c 20 b3 00 20 00 01 03 03 17 30 00 00 f3 11 4e File: "/home/user/Do gure4: ICMP 0. Time 2372 1.359855000 2380 1.364910000 2380 1.364910000 2398 1.377103000	68 50 c5 8d a5 11 00 74 01 5d 04 63 e4 00 00 00 00 45 71 c0 a8 00 01 63 wnloads/dat ■ Pack packet of tr Source 203.218.45.124 99.156.206.232 203.218.45.124	c0 08 00 45 00          3 96 a4 ca c0 a8          3 96 a4 ca 27 0f          3 96 a4 ca 27 0f          sets: 5809634 Displayed:          ype       3       (Destination)         ©       ●       ●         Destination       192,168.0.1         192,168.0.1       192,168.0.1         192,168.0.1       192,168.0.1		oad time: 1:01.707 chable) with co Chable) with co Apply mgth Info 74 Destination unreac 74 Destination unreac 74 Destination unreac	de 3 (Destinat	Profile: Default tion Port Uni	reachable
00       00       25       90       35       81         0       00       3       20       00       10       30       317         30       00       00       13       14       4         File: "/home/user/Do       gure4:       ICMP         Iter: icmp       Imp       Imp       Imp         2372       1.359855000       2380       1.364910000         2380       1.364910000       2402       1.3783110000         2419       1.3901640000       2419       1.3901640000	68 50 c5 8d a5 11 00 74 01 5d 04 63 e4 00 00 00 04 5 71 c0 a8 00 01 63 wnloads/dat Pack packet of to Source 203.218.45.124 99.156.206.232 203.218.45.124 202.140.51.162	C 0 08 00 45 00     3 96 a4 ca c0 a8     i 00 00 20 b0 51     96 a4 ca 27 0f     sets: 5809634 Displayed:     ype 3 (Destination		oad time: 1:01.707 <b>chable) with co</b> <b>i</b> Apply ngth Info 74 Destination unreac 74 Destination unreac 74 Destination unreac 74 Destination unreac 74 Destination unreac	de 3 (Destinat	Profile: Default tion Port Uni	reachable
00 00 25 90 35 81 10 00 3c 20 b3 00 20 00 01 03 03 17 30 00 00 f3 11 4e File: "/home/user/Do gure4: ICMP 0. Time 2372 1.359855000 2380 1.364910000 2398 1.377103000 2402 1.378311000 2419 1.390164000 2433 1.398453000	68 50 c5 8d a5 11 00 74 01 5d 04 63 e4 00 00 00 04 53 71 c0 a8 00 01 63 wnloads/dat Pack packet of tr Source 203.218.45.124 99.156.206.232 203.218.45.124 202.140.51.162 202.244.163.137	<ul> <li>C0 08 00 45 00</li></ul>		oad time: 1:01.707 chable) with co chable) with co interpretation of the second Apply ngth Info 74 Destination unreac 74 Destination unreac	de 3 (Destinat	Profile: Default tion Port Uni 2 % 2 1e) 1e) 1e) 1e) 1e) 1e) 1e) 1e)	reachable
00 00 25 90 35 81 10 00 3c 20 b3 00 20 00 01 03 03 17 30 00 00 f3 11 4e File: "/home/user/bo gure4: ICMP Iter: icmp b. Time 2372 1.359855000 2398 1.377103000 2402 1.378311000 2419 1.390164000 2433 1.394859000 2433 1.394859000 2435 1.39988000	68 50 c5 8d a5 11 00 74 01 5d 04 63 e4 00 00 00 04 55 71 c0 a8 00 01 63 wwnloads/dat Pack packet of ty Source 203.218.45.124 203.218.45.124 202.140.51.162 202.44.63.137 99.150.164.202 98.215.104.75	<ul> <li>c0 08 00 45 00, 3</li> <li>96 a4 ca c0 a8</li> <li>c0 00 02 0b 051, 3</li> <li>96 a4 ca 27 0f</li> <li>rets: 5809634 Displayed:</li> <li>ype 3 (Destination</li> <li>Pestination</li> <li>192,168.0.1</li> </ul>	S. hP E.     J. C	oad time: 1:01.707 <b>chable) with co</b> <b>chable) with co</b> <b>chable) with co</b> <b>chable) with co</b> <b>chable) with co</b> <b>chable chable chable</b> <b>chable chable</b> <b>chable chable</b> <b>chable chable</b> <b>chable chable</b> <b>chable chable</b> <b>chable chable</b> <b>chable chable</b> <b>chable chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>chable</b> <b>ch</b>	de 3 (Destinat	E Profile: Default tion Port Uni	reachable
00 00 25 90 35 81 10 00 3c 20 b3 00 20 00 01 03 03 17 30 00 00 f3 11 4e File: "/home/user/bo gure4: ICMP Iter: icmp 2372 1.359855000 2380 1.364910000 2398 1.377103000 2402 1.378311000 2419 1.390164000 2433 1.394853000 2433 1.394823000 2455 1.408238000 2455 1.408238000	68 50 c5 8d a5 11 00 74 01 5d 04 63 e4 00 00 00 04 63 71 c0 a8 00 01 63 wwnloads/dat ■ Pack packet of ty Dacket of ty Source 203.218.45.124 99.156.206.232 203.218.45.124 202.140.51.162 202.341.63.137 99.150.164.202 98.215.104.75 192.168.0.1	<ul> <li>c0 08 00 45 00, %</li> <li>3 96 a4 ca c0 a8, %</li> <li>3 96 a4 ca 27 0f</li> <li>3 96 a4 ca 27 0f</li> <li>ets: 5809634 Displayed:</li> <li>ype 3 (Destination</li> <li>192.168.0.1</li> </ul>		oad time: 1:01.707 <b>chable) with co</b> <b>chable) wit</b>	de 3 (Destinat a)  b)  b)  c)  c)  c)  c)  c)  c)  c)  c)  c)  c	E Profile: Default tion Port Uni 2 % 2 1e) 1e) 1e) 1e) 1e) 1e) 1e) 1e)	reachable
00 00 25 90 35 81 10 00 3c 20 b3 00 20 00 01 03 03 17 30 00 00 f3 11 4e File: "/home/user/Do gure4: ICMP 0. Time 2372 1.359855000 2380 1.364910000 2398 1.377103000 2402 1.37831000 2419 1.3901640000 2433 1.398459000 2433 1.398459000 2433 1.398459000 2435 1.408238000 2455 1.408238000 2455 1.408238000 2455 1.408238000	68 50 c5 8d a5 11 00 74 01 5d 04 63 e4 00 00 00 04 63 71 c0 a8 00 01 63 wwnloads/dat Pack packet of ty Source 203.218.45.124 90.156.206.232 203.218.45.124 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.164.202 98.215.104.75	<ul> <li>c0 08 00 45 00,</li> <li>3 96 a4 ca c0 a8,</li> <li>3 96 a4 ca 27 0f</li> <li>3 96 a4 ca 27 0f</li> <li>ets: 5809634 Displayed:</li> <li>ype 3 (Destination</li> <li>192,168,0,1</li> </ul>	S. hP E.     ] . C	oad time: 1:01.707 <b>chable) with co</b> <b>chable) wit</b>	de 3 (Destinat	E Profile: Default tion Port Unn 2 % 2 1e) 1e) 1e) 1e) 1e) 1e) 1e) 1e)	: reachable ltered)
00 00 25 90 35 81 00 00 25 90 35 81 00 00 10 30 317 00 00 07 311 4e File: "/home/user/Do gure4: ICMP 0. Time 2372 1.359855000 2380 1.364910000 2380 1.364910000 2398 1.377103000 2402 1.378311000 2419 1.391640000 2431 1.398459000 2431 1.398459000 2432 1.408238000 2435 1.408238000 2455 1.409247000 2462 1.409247000 2462 1.409247000 2465 1.410796000 2468 1.415550000 2469 1.433021000	68 50 c5 8d a5 11 00 74 01 5d 04 63 e4 00 00 00 04 63 71 c0 a8 00 01 63 wwnloads/dat Pack packet of t Source 203.218.45.124 99.156.206.232 203.218.45.124 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 202.140.51.162 203.218.45.124	<ul> <li>c0 08 00 45 00,</li> <li>3 96 a4 ca c0 a8,</li> <li>3 96 a4 ca 27 0f,</li> <li>3 96 a4 ca 27 0f,</li> <li>3 96 a4 ca 27 0f,</li> <li>cets: 5809634 Displayed:</li> <li>ype 3 (Destination</li> <li>192.168.0.1</li> </ul>	S. hP E.     ] . C	oad time: 1:01.707 <b>chable) with co</b> <b>chable) wit</b>	de 3 (Destinat	Profile: Default tion Port Uni	: reachable



<b>i</b> (	i 🖭 🔍 1	🏟   📔 🖾 🗙 C	🚊   Q 🔶 🤿	<b>↓ ₹ ⊥</b>	🗐 💽 🖕 🗉 🕅 🔛 🔛 🔀 🔀 🔇
Filter:	icmp		Expression	ssion Clear	Apply
No.	Time	Source	Destination	Protocol Le	ngth Info
158	9 0 961686000	0 99 29 79 36	192.168.0.1	TCMP	70 Destination unreachable (Communication administratively filtered)
159	2 0.965316000	0 99.150.164.202	192.168.0.1	TCMP	74 Destination unreachable (Port unreachable)
1596	6 0.967381000	0 99.156.206.232	192.168.0.1	TCMP	74 Destination unreachable (Port unreachable)
1608	8 0.974086000	0 203.218.45.124	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
1609	9 0.975066000	0 99,150,164,202	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
161	7 0.979676000	0 192.168.0.1	200.196.50.249	ICMP	590 Destination unreachable (Port unreachable)
1623	2 0.981248000	0 99.29.79.36	192.168.0.1	ICMP	70 Destination unreachable (Communication administratively filtered)
1628	8 0.985755000	0 99.150.164.202	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
163	1 0.987270000	0 99.156.206.232	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
1640	0 0.995175000	0 203.218.45.124	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
164	5 0.997974000	0 99.150.164.202	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
166	7 1.010158000	0 99.150.164.202	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
167	5 1.013983000	0 99.156.206.232	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
1689	9 1.022240000	0 203.218.45.124	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
1693	3 1.022834000	0 99.29.79.36	192.168.0.1	ICMP	70 Destination unreachable (Communication administratively filtered)
▶ Frame	1622: 70 by	tes on wire (560 bits)	. 70 bytes captured (5	60 bits)	
▶ Ether	net II. Src:	JuniperN a5:11:c0 (50	:c5:8d:a5:11:c0). Dst:	SuperMic 35	:81:68 (00:25:90:35:81:68)
▶ Interr	net Protocol	Version 4. Src: 99.29	.79.36 (99.29.79.36).	Dst: 192.168	3.0.1 (192.168.0.1)
▼ Inter	net Control I	Message Protocol	,,		
Type	e: 3 (Destina	ation unreachable)			
Code	: 13 (Commun	nication administrative	ly filtered)		
Chec	ksum: 0xd5c5	[correct]	· · · ·		
▶ Inte	ernet Protoco	ol Version 4, Src: 192.	168.0.1 (192.168.0.1)	, Dst: 99.29.	.79.36 (99.29.79.36)
▶ User	Datagram Pr	otocol, Src Port: dist	inct (9999), Dst Port	: chargen (19	9)

0000	00 25 90 35 81 68 50 c5	8d a5 11 c0 08 00 45 00	.%.5.hPE.	
0010	00 38 15 37 00 00 f3 01	3f a3 63 1d 4f 24 c0 a8	.8.7 ?.c.0\$	
0020	00 01 03 0d d5 c5 00 00	00 00 45 00 00 20 cf cc	E	
0030	00 00 f4 11 84 15 c0 a8	00 01 63 1d 4f 24 27 0f		
	the second second second			
🔴 Fi	le: "/home/user/Downloads/da	at Packets: 5809634 Display	red: 197190 Marked: 0 Load time: 1:01.707	Profile: Default

Figure 6: ICMP packet of type 3 (Destination Unreachable) with code 13 (Communication administratively filtered)

The UDP flood consisted of many fragmented IP packets. For all of them, the protocol field was set to UDP and for most of them either the MF flag was set or the fragment offset was greater than zero.

Help participants by explaining the filters presented below. If participants have problems with finding the solution, provide the proper Wireshark.

Filters which could be used for this analysis are the Wireshark display filter, and the tcpdump filter.

Wireshark display filter: (udp && not udp.port == 53) || ip.flags.mf == 1 || ip.frag offset > 0

This is a sample Wireshark display filter allowing us to separate DDoS UDP flood. To do this we select all packets matching a) or b) or c) rule:

- a) (udp && not.udp == 53) all udp packets with port other than 53 (we're not interested in DNS traffic which isn't part of DDoS attack)
- b) ip.flags.mf == 1 packets having IP flag MF (More Frag.) set
- c) ip.frag\_offset > 0 packets with fragment offset greater than 0.

Tcpdump filter: ip[6:2]&8191>0 or ip[6]&32!=0 or (udp and not port 53)<sup>10</sup>

The second filter is the same filter, but written in BPF tcpdump filter syntax. This time we can't refer to separate fields of IP or UDP headers. To filter packets by IP header fields values we must refer to IP

<sup>&</sup>lt;sup>10</sup> ip[6:2]&8191>0 is for checking IP fragment offset field (2 bytes length starting from 6th byte of IP hdr, counting from 0)

ip[6]&32!=0 is for checking whether MF (More fragments) flag was set



header as byte array with ip[0] being a first byte of IP header. Syntax is as follows: ip[a:n] - 'n' bytes starting from 'a' position/element/byte. & operator denotes bitwise AND operation. a) ip[6:2]&8191>0 - fragment offset greater than 0 b) ip[6]&32!=0 - flag MF is set c) udp and not port 53 - all udp packets with port other than 53

Packets to port 53 are excluded as packets sent to this port were proper DNS requests and weren't part of DDoS attack (at least in this case).

8	🎒 🎒 📦 🗎 🛅	🛚 🗶 🤁 🚊 🔍 🔶 🗉	> 🗣 🖣 🖡 🗎		🏹 🗹 ங 🔀 🕐		
Filter:	not udp.port ==53    ip.flags.	mf == 1    ip.frag_offset > 💌 E	xpression Clear Apply				
No.	Time Source	Destination	Protocol Length Info				
3452	1.970980000 200.145.156	.238 192.168.0.1	UDP 1514 Sour	ce port: chargen Des	tination port: distinct		
3454	1.972579000 200.145.25.	26 192.168.0.1	UDP 1514 Sour	ce port: chargen Des	tination port: distinct		
3460	1.975467000 99.29.79.36	192.168.0.1	ICMP 70 Des	ination unreachable (	Communication administrat	ively filtered)	
3461	1.977129000 99.29.79.36	192.168.0.1	ICMP 70 Des	ination unreachable (	Communication administrat	ively filtered)	
3470	1.978669000 68.85.179.1	70 192.168.0.1	ICMP 70 Des	ination unreachable (	Host unreachable)		
3473	1.980085000 99.150.164.	202 192.168.0.1	ICMP 74 Des	ination unreachable (	Port unreachable)		
3480	1.986712000 203.218.45.	124 192.168.0.1	ICMP 74 Dest	ination unreachable (	Port unreachable)		
3489	1.990863000 200.145.25.	26 192.168.0.1	UDP 1514 Sour	ce port: chargen Des	tination port: distinct		
3493	1.992277000 203.218.45.	124 192.168.0.1	ICMP 74 Des	ination unreachable (	Port unreachable)		
3494	1.992330000 99.150.164.	202 192.168.0.1	ICMP 74 Des	ination unreachable (	Port unreachable)		
3495	1.992963000 200.145.156	.238 192.168.0.1	UDP 1514 Sour	ce port: chargen Des	tination port: distinct		
3496	1.996105000 200.143.210	.11 192.168.0.1	UDP 1208 Sour	ce port: chargen Des	tination port: distinct		
3499	1.996437000 200.196.50.	249 192.168.0.1	UDP 1329 Sour	ce port: chargen Des	tination port: distinct		
3500	1.996468000 192.168.0.1	200.196.50.249	ICMP 590 Des	ination unreachable (	Port unreachable)		
3501	1.997002000 200.145.78.	193 192.168.0.1	UDP 1514 Sour	ce port: chargen Des	tination port: distinct		
▼ Interne	et Protocol Version 4. S	Src: 200.145.156.238 (200.14	5,156,238), Dst: 192,168	.0.1 (192.168.0.1)	Port Unreachable)		
Versi	on: 4						
Heade	r length: 20 bytes						
▶ Diffe	rentiated Services Field	d: 0x00 (DSCP 0x00: Default;	; ECN: 0x00: Not-ECT (Not	ECN-Capable Transport	t))		
Total	Length: 1500						
Ident	ification: 0x652b (25899	9)					
▶ Flags	: 0x01 (More Fragments)						
Fragm	ent offset: 0						
Time	to live: 108						
Proto	col: UDP (17)						
▶ Heade	r checksum: 0x9dbc [cori	rect]					
Sourc	e: 200.145.156.238 (200	.145.156.238)					
Desti	nation: 192.168.0.1 (192	2.168.0.1)					
0000 00	25 90 35 81 68 50 c5 8	3d a5 0e 80 08 00 45 00 .9	6.5.hPE.				
0010 05	dc 65 2b 20 00 6c 11 9	9d bc c8 91 9c ee c0 a8	.e+ .l				
0020 00	01 00 13 27 0f 0e 71 f	Fc d1 20 21 22 23 24 25	' a I"#\$%				
0000	1020 00 01 00 13 27 0f 0e 71 fc d1 20 21 22 23 24 25,'.q., !##%%						
0030 26	27 28 29 2a 2b 2c 2d 2	2e 2f 30 31 32 33 34 35 &	'()*+,/012345				
0030 26	27 28 29 2a 2b 2c 2d 2 home/user/Downloads/data	2e 2f 30 31 32 33 34 35 & a_(= Packets: 5809634 Displayed:	2341296 Marked: 0 Load time	: 1:34.740	E Profil	e: Default	

Figure 7: Excluded packets to port 53 that are legitimate packets



🗐 🎘 🗐 😂 🍏 I 🛅 🖂 🗙 🔇	; 🚊 🔍 🔶 🚽	<b>ə</b> 7	🛓 🗐 🖬 c – c 🖭 🕁 🕅 🐚 💥 📀					
Filter: udp && not udp.port ==53    ip.flags.mf	== 1    ip.frag_o 🔻 Exp	oression Cl	ear Apply					
No. Time Source	Destination	Protocol	Length Info					
2441472 550.2002510(90.25.121.05	192.100.0.1	UUF	1514 Source port, chargen bestination port, distinct					
2441473 350.2683520(98.215.157.124	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct					
2441476 350.2684720(206.212.241.250	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct					
2441477 350.2684840(202.142.218.218	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct					
2441485 350.2689770(200.155.21.125	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct					
2441486 350.2690180(101.140.18.78	192.168.0.1	UDP	1490 Source port: chargen Destination port: distinct					
2441491 350.2692870(203.68.179.85	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct					
2441492 350.2693220(98.223.66.157	192.168.0.1	UDP	715 Source port: chargen Destination port: distinct					
2441493 350.2694250(203.94.64.17	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct					
2441495 350.2696480(202.143.146.108	192.168.0.1	UDP	1123 Source port: chargen Destination port: distinct					
2441497 350.2697460(200.198.193.174	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct					
2441498 350.2698030(200.208.204.102	192.168.0.1	UDP	1514 Source port: hdap Destination port: distinct					
2441499 350.2698160(98.223.214.14	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct					
2441500 350.2698190(200.91.233.61	192.168.0.1	UDP	131 Source port: chargen Destination port: distinct					
2441501 350.2698920(202.157.179.209	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct					
2441502 350.2699360(203.135.192.130	192.168.0.1	UDP	1466 Source port: chargen Destination port: distinct					
▼ Internet Protocol Version 4, Src: 98.2	3.121.83 (98.23.121.)	83), Dst: 19	02.168.0.1 (192.168.0.1)					
Version: 4								
Header length: 20 bytes								
▶ Differentiated Services Field: 0x00 (	DSCP 0x00: Default:	ECN: 0x00: N	Not-ECT (Not ECN-Capable Transport))					
Total Length: 1500								
Identification: 0x377c (14204)								
▼ Flags: 0x01 (More Fragments)								
0 = Reserved bit: Not set								
.0 = Don't fragment: Not set								
1 = More fragments: Set								
Fragment offset: 0								
Time to live: 111								
Protocol: UDP (17)	I me to I type: III							
	17 70 50 -0 -0 -							
0010 05 dc 37 /c 20 00 6f 11 52 81 62	1/ /9 53 c0 a8/	.o. R.b.ys	5 ###					
0030 26 27 28 29 2a 2b 2c 2d 2e 2f 30	21 22 23 24 23 31 32 33 34 35 &'(	)*+/0123	74 M 345					
0040 36 37 38 39 3a 3b 3c 3d 3e 3f 40	41 42 43 44 45 678	9:;<= >?@ABC	TDE					
More fragments (in flags mf) 1 h = Backe	te: E800624 Displayed: 2	241206 Marko	d: 01 ood time: 1:24 740					
more regine its (pritegs int), to reckets, sovoor bispaged, control with each of the control of the co								

Figure 8: UDP packet with More Fragments (MF) bit set

Next, participants should recognise what distinct streams the DDoS attack consisted of (either different attack methods/techniques or clear source distinction). They can analyse input/output statistics for those streams in comparison with normal server traffic. To complete this task they should:

- 1. open the PCAP file in Wireshark;
- 2. choose Statistics  $\rightarrow$  IO Graph;
- 3. use the display filters created in the previous point to create separate graphs;
- 4. adjust other options if needed (X and Y axis scale, line style, etc.)



\*\*\*\* \* enisa \*\*\*\*

September 2014



Figure 9: statistics of the initial DDoS phase.

Figure 9 presents the initial phase of the DDoS attack. Legitimate HTTP traffic is marked with a red line. We can see strong fluctuations over time of this type of traffic (which is quite normal). DDoS traffic (UDP flood) is marked with a pink line. In this case, fluctuations are much smaller and its throughput is almost constant (~10 Mbps). Also we can see that DDoS traffic doubles the average throughput of HTTP traffic.



Figure 10: Slight increase of ICMP traffic (blue line) with the start of the second DDoS phase

Figure 10 presents a slight increase of value for ICMP traffic around 14:18:00. This increase is a representation of the second phase of the DDoS attack.





#### Figure 11: Second DDoS phase

Around 14:17:58, the second DDoS phase started. We can see that with the start of the second DDoS phase, the total traffic significantly increased. Total traffic throughput increased from ~22.5 Mbps to ~200 Mbps, which means that traffic increased nearly nine times in comparison with the first phase, and forty times in comparison with legitimate HTTP traffic (~5Mbps). We should also note that traffic increase was almost entirely due to UDP flood (green line).



Figure 12: Second DDoS phase in detail



Figure 12 more clearly shows us increase of UDP flood (green line) traffic with the beginning of the second DDoS phase.

The next subtask for participants is to determine the endpoints' addresses of analysed hosts. There are various ways to export such addresses – they can do this using either Wireshark or tcpdump.

#### Method 1 with Wireshark:

If participants use Wireshark application they should follow the following steps.

- 1. Open pcap with DDoS traffic in Wireshark (alternatively just apply the proper display filter to the file with all captured traffic).
- 2. Choose Statistics  $\rightarrow$  Endpoints and switch to IPv4 tab.

				IPv4 Endpoints							
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude			
10.157.5.204	4 401	2 330 335	2 500	334 389	1 901	1 995 946		-			
192.168.0.1	5 436 937	5 955 477 201	321 809	268 372 725	5 115 128	5 687 104 476		-			
10.230.46.182	1 082	559 146	684	71 411	398	487 735		-			
10.14.148.186	443	218 516	251	55 983	192	162 533		-			
99.29.79.36	13 344	934 080	6 672	467 040	6 672	467 040		-			
200.150.68.218	16 244	18 122 259	15 892	17 979 650	352	142 609		-			
203.218.45.124	41 624	3 080 176	20 812	1 540 088	20 812	1 540 088		-			
99.150.164.202	40 208	2 975 392	20 104	1 487 696	20 104	1 487 696		-			
200.196.50.249	24 646	30 120 777	24 294	29 945 808	352	174 969		-			
200.137.128.25	24 950	30 491 811	24 601	30 315 773	349	176 038		-			
99.156.206.232	34 238	2 533 612	17 119	1 266 806	17 119	1 266 806		-			
200.128.79.52	25 764	31 717 867	25 412	31 542 774	352	175 093		-			
200.136.91.11	24 879	30 707 637	24 528	30 534 219	351	173 418		-			
202.5.131.5	24 862	30 298 864	24 510	30 125 999	352	172 865		-			
10.27.121.68	31	3 338	10	564	21	2 774		-			
203.81.218.138	6 945	7 115 964	6 605	6 995 080	340	120 884		-			
200.145.25.26	25 389	31 287 228	25 041	31 111 144	348	176 084		-			
203.94.64.17	16 612	20 092 922	16 264	19 940 558	348	152 364		-			
200.133.238.11	14 465	16 211 320	14 118	16 084 428	347	126 892		-			
200.145.156.238	47 642	58 705 180	47 292	58 525 100	350	180 080		-			
200.143.210.11	24 855	30 385 347	24 503	30 208 606	352	176 741		-			

Figure 13 Sources of the DDoS attack and packets statistics

- 3. If necessary make sure the 'Limit to display filter' option is selected.
- 4. Click 'Copy' and paste the data to some file. The data is in CSV format.
- 5. Save file as ddos.csv
- 6. Get the ip addresses only from .csv file using the following command:
  - cat ddos.csv | cut -d '"' -f 2 > ddos ip.uniq

#### Method 2 with tcpdump

If participants want to use tcpdump they should follow the following steps.

- 1. Use the tcpdump command:
  - tcpdump -n -r data ddos.pcap '<filter>'

As the result they should receive:





14:13:28.944879 IP 99.29.x.x > 92.158.x.x: ICMP host 99.29.79.36 unreachable - admin prohibited filter, length 36

14:13:28.947665 IP 203.218.x.x > 92.158.x.x: ICMP 203.218.45.124 udp port 19 unreachable, length 40

14:13:28.948177 IP 99.29.x.x > 92.158.x.x: ICMP host 99.29.79.36 unreachable - admin prohibited filter, length 36

14:13:28.951068 IP 99.150.x.x > 92.158.x.x: ICMP 99.150.164.202 udp port 19 unreachable, length 40 2. Use the tcpdump command:

tcpdump -n -r ddos.pcap | perl -ne 'if (m/IP
 (\d+\.\d+\.\d+\.\d+)/){print "\$1\n";}' | sort -u >
 ddos ip.uniq

This should produce the list of unique IP addresses (ddos\_ip.uniq). Such list can be used for finding more information, e.g. autonomous systems. To get list of autonomous systems associated with these addresses, participants can use the free service available at The Shadowserver Foundation: <a href="http://www.shadowserver.org/wiki/pmwiki.php/Services/IP-BGP">http://www.shadowserver.org/wiki/pmwiki.php/Services/IP-BGP</a>

All information gathered during the subtasks should be used to prepare the full report (see Task 3).

#### 3.4 Task 3: Evaluating countermeasures values

After collecting all information from network monitoring data, participants should prepare a security incident report for the national regulatory authority (NRA). To better prepare this report, they should first learn more about the reporting schema template. You should present them the template and explain its fields using the following guide from the ENISA document *Technical Guide on Reporting Incidents*.<sup>11</sup> Each participant should use one of the ISP providers that they are most familiar with. The name of the ISP can be fictitious. Keeping in mind and referring to the real examples from their countries gives participants an additional chance to exchange information about practical aspects of cooperation between CERTs and ISPs in different countries. There is no need to use real names for this purpose.

Field	Description	Tip for fulfilling
Country	The country that sends the report to NRA	
Date and time	Details of the date and time when the incident took place (in national time). It can be interpreted as the time the incident was discovered.	According to analysed logs

<sup>&</sup>lt;sup>11</sup> (http://www.enisa.europa.eu/activities/Resilience-and-

<sup>&</sup>lt;u>CIIP/Incidents%20reporting/Technical%20Guidelines%20on%20Incident%20Reporting/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting) (page 20).</u>



	Time should be expressed in both CET and local time.		
Impacted services	The affected service: the service rendered unavailable to the end- user. This field includes a description of the service whose continuity and availability are affected by the impact level. It should be noted that assessing the Level of Service (LoS) Quality of Service (QoS) introduces complexity into the analysis criteria and can become subjective. The possible choice is: fixed telephony, mobile telephony, (short) message services, Internet, email.	According to participants' knowledge of online service functionality and services	
Number of users affected	The total number of users affected when an incident occurs (percentage of all affected users of that service in a given country). The national report to the NRA may include the absolute number the NRA would have to translate into percentages for inclusion in the annual report to ENISA and the European Commission.	According to participants' knowledge of online service functionality and services	
Duration	The duration of the incidents	According to analysed logs	
Geographic spread/region	If available, the region impacted by the incident	According to the participants' choice of ISP geographical location. Add information about geographical location of attacking parties.	
Impact on Emergency calls	If available emergency service impacted by the incident	For the purpose of the exercise, the real data of CERTs represented by participants	
Description	Fill in any further information you can share on the impact of the incident.	According to the findings from logs analysis	



Root cause	What kind of disaster or reason caused the security problem. The potential choices are: natural disaster or phenomena, human error, malicious attack, hardware or software failure, failure at third party or external party.	According to participants' knowledge of the source of incident. The description and findings can be changed during the analysis.
Other incident information	A general description of the incident. Also the description of all the incident handling actions and activities undertaken by a handler and post-incident actions. In this part of the report, there is information about other possible parties affected by an incident. Other descriptive information about an incident includes lessons learnt from an incident and further remarks. There is one more particular piece of information requested – NRA's contacted (in case of a cross –border incident). This one is especially dedicated for the NRA. From the perspective of the ISP and its CERT it is included in information about cooperation and contact with other parties.	

Some of the information is not very important in preparing the report in terms of the exercise purposes, but it is important to give participants the whole picture and mention and discuss all information.<sup>12</sup>

#### 4 Summary of the exercise

In the summary ask participants to present their findings about the incident by presenting the requested fields of the security incident report. Be sure that all participants present their work results. In particular, discuss findings if they differ among participants. Find a proper solution.

At the end of the summary, present again the main rules for incident reporting schema between ISPs, NRAs and ENISA and explain the purposes of these regulations, as well as benefits for CERTs. These benefits may include:

closer cooperation between CERTs on the operational level;

<sup>&</sup>lt;sup>12</sup> More descriptions of the report fields are available in the ENISA document 'Technical Guideline on Reporting Incidents – Article 13a Implementation' (page 21). <u>https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-for-incident-reporting-v1.0</u>



- common schema for collecting information about incidents;
- closer cooperation inside each Member States between parties involved in improving security level;
- systematic collection of security incident related data and its usage for building awareness about security threats in the Internet;



#### ENISA

European Union Agency for Network and Information Security Science and Technology Park of Crete (ITE) Vassilika Vouton, 700 13, Heraklion, Greece

#### **Athens Office**

1 Vass. Sofias & Meg. Alexandrou Marousi 151 24, Athens, Greece



PO Box 1309, 710 01 Heraklion, Greece Tel: +30 28 14 40 9710 info@enisa.europa.eu www.enisa.europa.eu