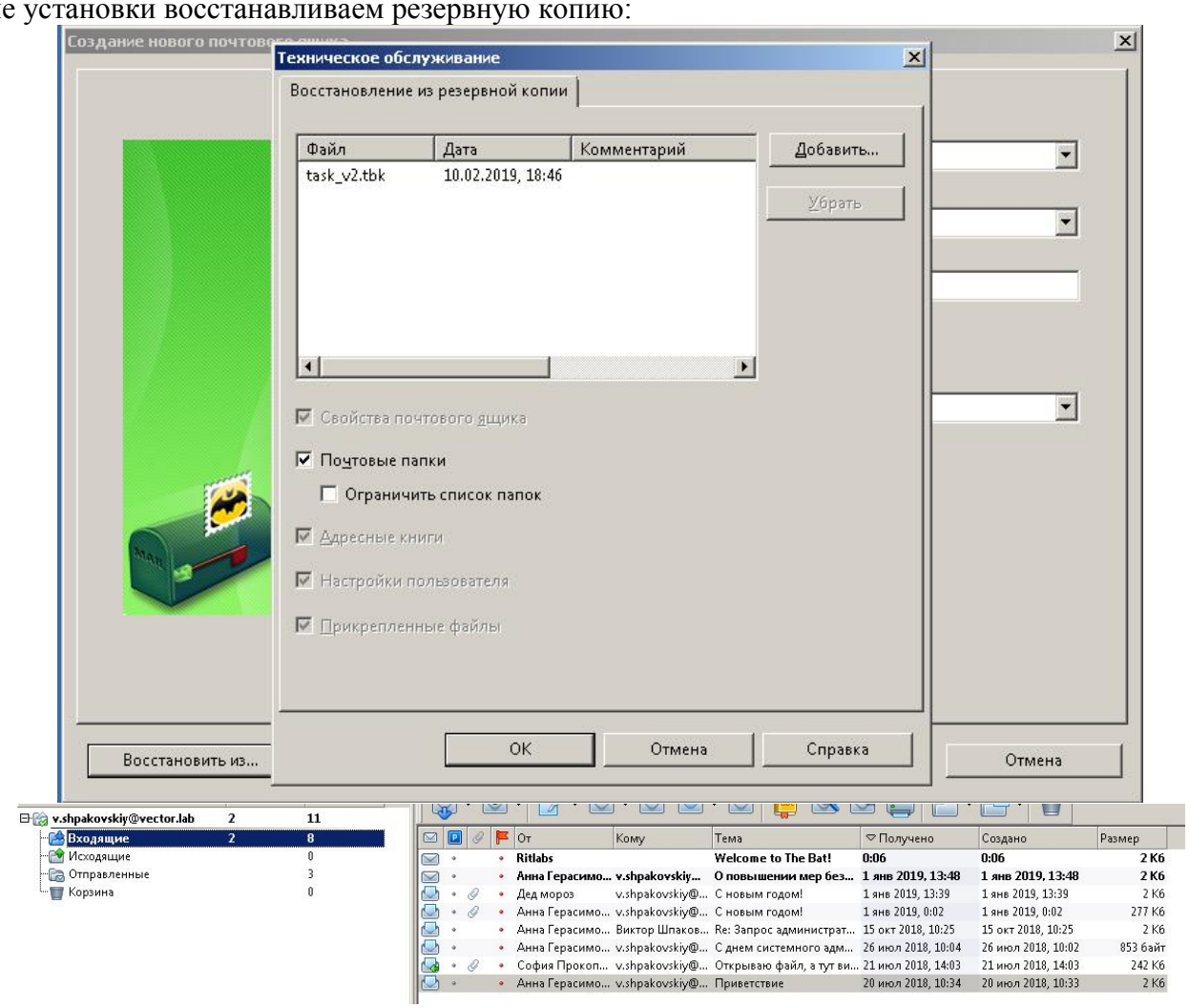
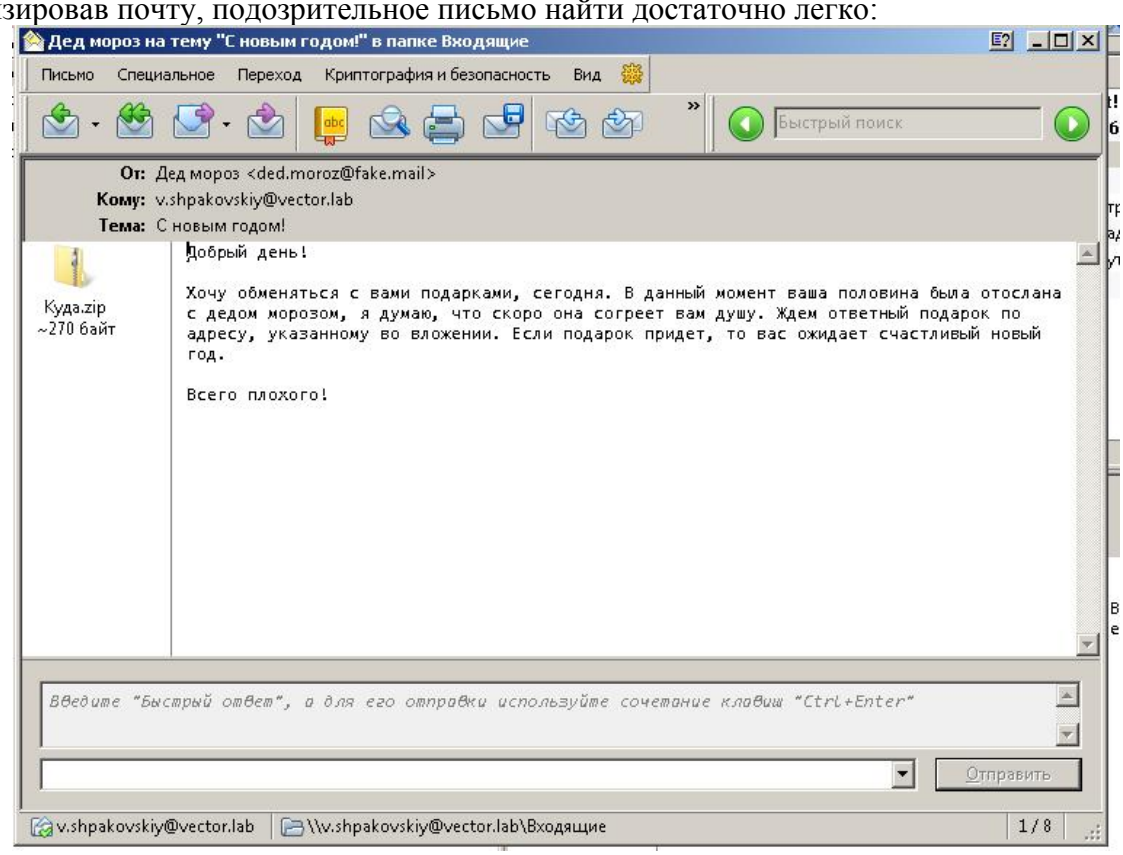
В описании к заданию есть намек на почтовую программу “The Bat!”. Файл является резервной копией почтового ящика (всё можно нагуглить).
После установки восстанавливаем резервную копию:

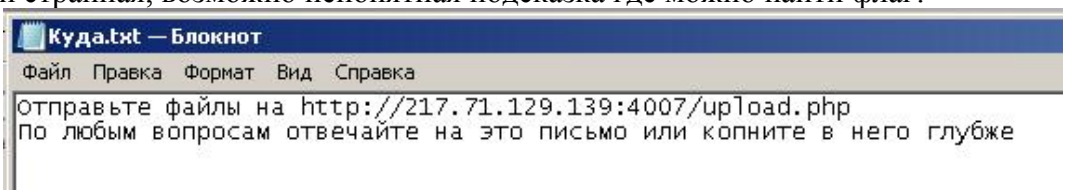


Проанализировав почту, подозрительное письмо найти достаточно легко:



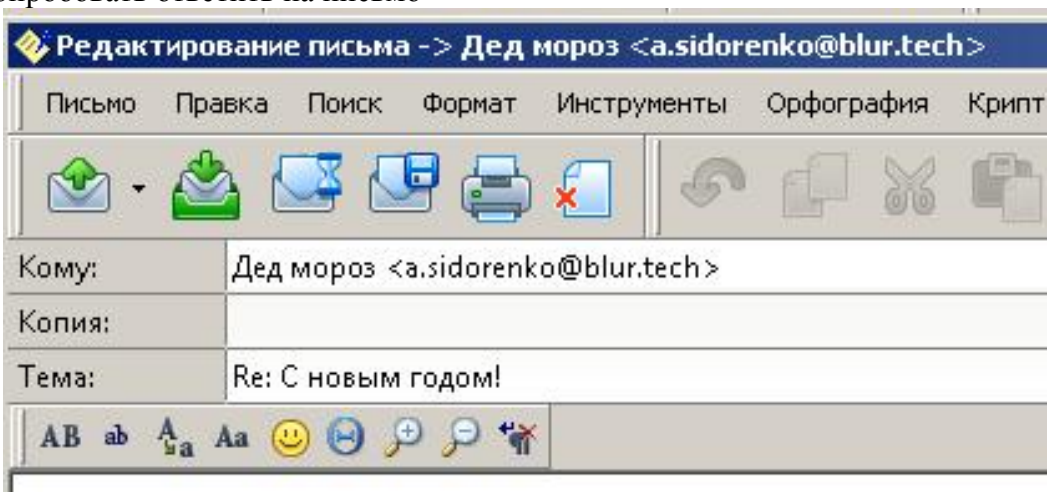
fake.mail подразумевает, что это не та почта, которая нужна.

Во вложении странная, возможно непонятная подсказка где можно найти флаг:

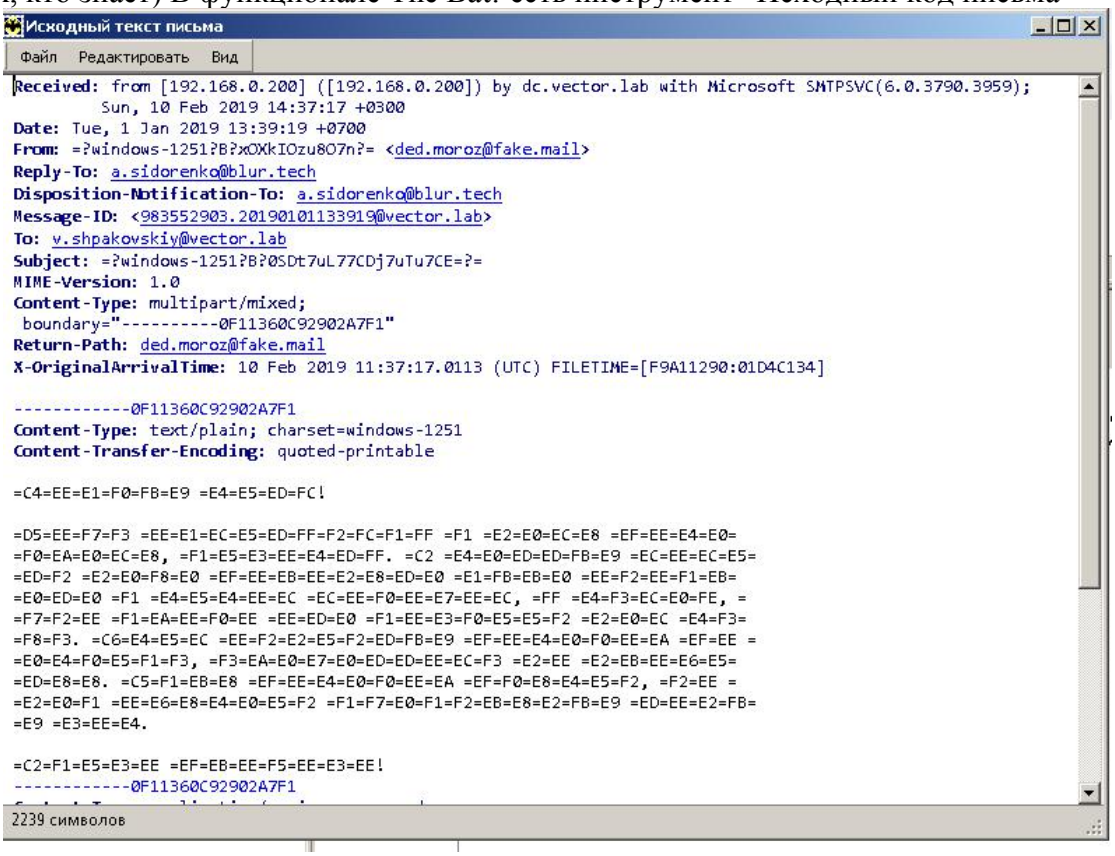


Тут 2 варианта:

1. Можно попробовать ответить на письмо



2. (для тех, кто знает) В функционале The Bat! есть инструмент “Исходный код письма”



Вариант решения через трафик:

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	18152	100,00 %	13773104	0,347	0	0	0,000
Ethernet	100,00 %	18152	1,85 %	254128	0,006	0	0	0,000
Internet Protocol Version 4	99,62 %	18083	2,63 %	361680	0,009	0	0	0,000
Transmission Control Protocol	93,81 %	17028	94,69 %	13041288	0,328	10528	5980701	0,151
Secure Sockets Layer	28,44 %	5163	80,12 %	11035110	0,278	5062	9179994	0,231
Data	1,53 %	277	1,68 %	230868	0,006	277	231503	0,006
Post Office Protocol	0,10 %	18	0,03 %	4015	0,000	17	3950	0,000
Internet Message Format	0,01 %	1	0,00 %	65	0,000	1	65	0,000
Simple Mail Transfer Protocol	0,09 %	17	0,06 %	8040	0,000	16	4881	0,000
Internet Message Format	0,01 %	1	0,05 %	7320	0,000	1	7320	0,000
Hypertext Transfer Protocol	1,13 %	206	4,07 %	560950	0,014	93	35827	0,001
Line-based text data	0,25 %	46	1,54 %	212272	0,005	46	96146	0,002
Online Certificate Status Protocol	0,06 %	10	0,04 %	4932	0,000	10	4932	0,000
JPEG File Interchange Format	0,02 %	3	0,59 %	80574	0,002	3	81561	0,002
JavaScript Object Notation	0,02 %	3	0,00 %	234	0,000	3	805	0,000
Media Type	0,05 %	9	0,12 %	16740	0,000	9	10618	0,000
Compuserve GIF	0,04 %	7	0,01 %	1824	0,000	7	1824	0,000
HTML Form URL Encoded	0,01 %	2	0,00 %	678	0,000	2	678	0,000
Portable Network Graphics	0,01 %	2	0,42 %	57204	0,001	2	57670	0,001
MIME Multipart Media Encapsulation	0,08 %	15	0,53 %	73655	0,002	15	77010	0,002
eXtensible Markup Language	0,07 %	12	0,50 %	68729	0,002	12	70142	0,002
Telnet	5,04 %	914	0,56 %	76653	0,002	914	76653	0,002
Malformed Packet	0,06 %	10	0,00 %	0	0,000	10	0	0,000
User Datagram Protocol	5,75 %	1043	0,06 %	8344	0,000	0	0	0,000
Multicast Domain Name System	0,01 %	1	0,00 %	118	0,000	1	118	0,000
Mikrotik Neighbor Discovery Protocol	0,03 %	5	0,00 %	515	0,000	5	515	0,000
Bootstrap Protocol	0,03 %	6	0,01 %	1805	0,000	6	1805	0,000

Help Close

В трафике находятся 2 протокола, относящиеся к почте: POP и SMTP. В сессии POP3:

Follow TCP Stream (tcp.stream eq 6)

Stream Content

```
34 20190210143717011300000008
.
+OK 2241 octects
Received: from [192.168.0.200] ([192.168.0.200]) by dc.vector.lab with Microsoft
SMTPSVC(6.0.3790.3959);
. Sun, 10 Feb 2019 14:37:17 +0300
Date: Tue, 1 Jan 2019 13:39:19 +0700
From: =?windows-1251?B?xOXkIOzu8O7n?= <ded.moroz@fake.mail>
Reply-To: a.sidorenko@blur.tech
Disposition-Notification-To: a.sidorenko@blur.tech
Message-ID: <983552903.20190101133919@vector.lab>
To: v.shpakovskiy@vector.lab
Subject: =?windows-1251?B?0SDt7uL77CDj7uTu7CE=?=
MIME-Version: 1.0
Content-Type: multipart/mixed;
 boundary="----------0F11360C92902A7F1"
Return-Path: ded.moroz@fake.mail
X-OriginalArrivalTime: 10 Feb 2019 11:37:17.0113 (UTC) FILETIME=[F9A11290:01D4C134]

------------0F11360C92902A7F1
Content-Type: text/plain; charset=windows-1251
```

Entire conversation (4015 bytes)

Find Save As Print ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ◉ Raw

Help Filter Out This Stream Close

Флаг: **CTF{a.sidorenko@blur.tech}**