

BASIC E-MAIL ANALYSIS

topics

- **e-mail spoofing**
- **intro to e-mail forensics (e-mail tracking)**

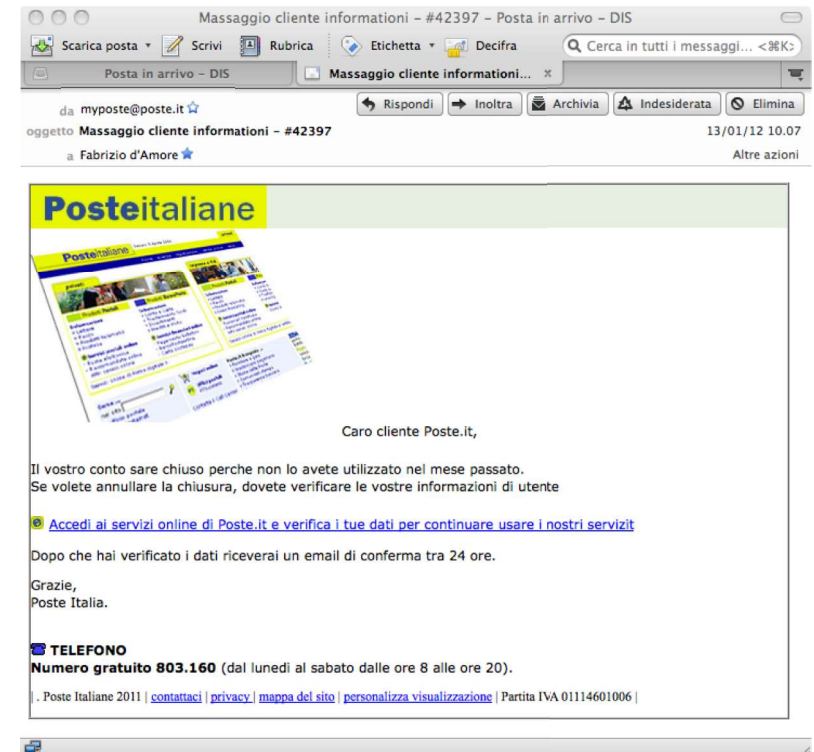
E-MAIL SPOOFING

- activity of altering the e-mail's sender address to the purpose of making the message looking like originated from other sender
 - the spoofer will possibly alter other fields
- easy in the plain Internet e-mail system, since original SMTP doesn't provide any authentication
 - later, a few mechanisms for authentication have been introduced, such as SMTP-AUTH
- most of spam/phishing e-mail messages are spoofed

A TYPICAL EXAMPLE

```
Sorgente di: imap://damore@imap.dis.uniroma1.it:993/fetch%3EUID%3E/Junk%3E47620

Return-Path: <root@periscope.hu>
X-Original-To: damore@dis.uniroma1.it
Delivered-To: damore@dis.uniroma1.it
Received: from localhost (webmail.dis.uniroma1.it [151.100.59.69])
    by mail.dis.uniroma1.it (Postfix) with ESMTP id B7AB628203
    for <damore@dis.uniroma1.it>; Fri, 13 Jan 2012 10:14:32 +0100 (CET)
Received: from webmail.dis.uniroma1.it ([127.0.0.1])
    by localhost (webmail [127.0.0.1]) (amavisd-new, port 10024) with ESMTP
    id 08099-11 for <damore@dis.uniroma1.it>;
    Fri, 13 Jan 2012 10:14:29 +0100 (CET)
Received: from morpheus.periscope.hu (shosting-26.84.nethub.hu [87.229.26.84])
    by webmail.dis.uniroma1.it (Postfix) with ESMTP id DBC23154AA1
    for <damore@dis.uniroma1.it>; Fri, 13 Jan 2012 10:14:28 +0100 (CET)
Received: by morpheus.periscope.hu (Postfix, from userid 0)
    id B3108A147102; Fri, 13 Jan 2012 10:07:01 +0100 (CET)
To: damore@dis.uniroma1.it
Subject: Massaggio cliente informazioni - #42397
From: myposte@poste.it
Content-Type: text/html
Message-Id: <20120113090701.B3108A147102@morpheus.periscope.hu>
```



SIMPLE SPOOFING SESSION

```
telnet mail.dis.uniroma1.it 25
Trying 151.100.59.100...
Connected to mail.dis.uniroma1.it.
Escape character is '^]'.
220 Mail Server ESMTTP
helo babbonatale
250 mail.dis.uniroma1.it
mail from:<Babbo.Natale@NorthPole.Earth>
250 Ok
rcpt to:<damore@dis.uniroma1.it>
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
Message-ID: 4F525268.40304@NorthPole.Earth
Date: Sat, 03 Mar 2012 18:18:32 +0100
From: Babbo Natale
<Babbo.Natale@NorthPole.Earth>
```

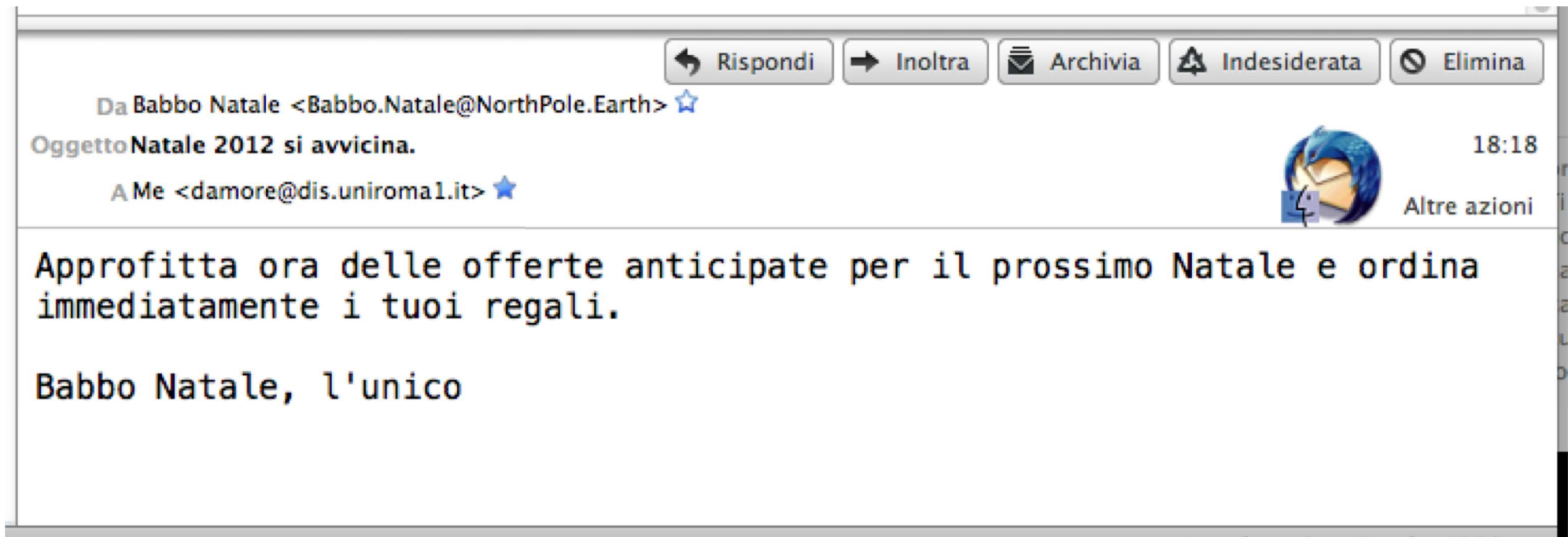
```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac
OS X 10.7; rv:10.0.2) Gecko/20120216
Thunderbird/10.0.2
MIME-Version: 1.0
To: Fabrizio d'Amore <damore@dis.uniroma1.it>
Subject: Natale 2012 si avvicina.
Content-Type: text/plain; charset=ISO-8859-15
Content-Transfer-Encoding: 7bit
```

Approfitta ora delle offerte anticipate per il prossimo Natale e ordina immediatamente i tuoi regali.

Babbo Natale, l'unico

```
.
250 Ok: queued as AF3B722FDD
quit
221 Bye
Connection closed by foreign host.
```

SPOOFING RESULT

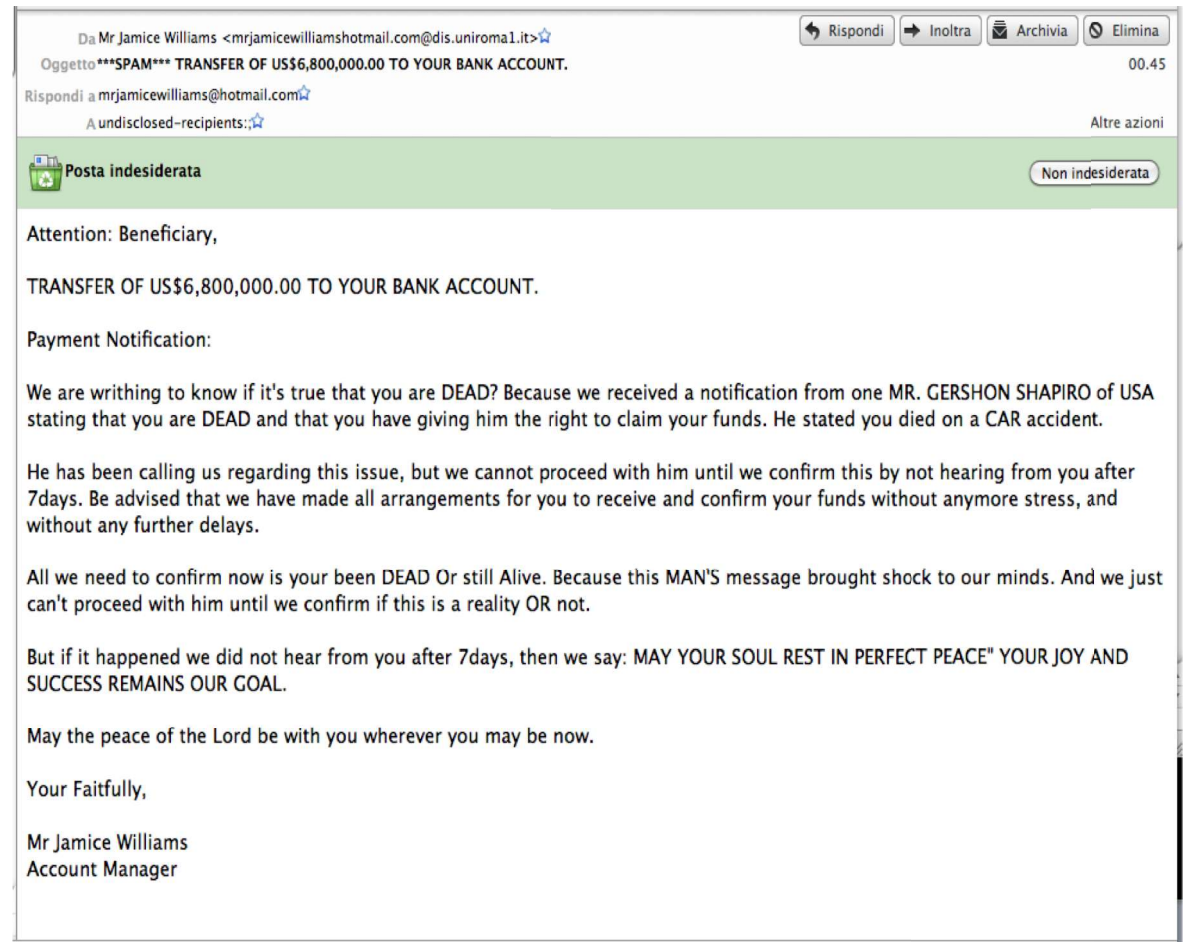


HOW TO CHECK FOR SPOOFING

- no success-guaranteeing techniques
 - it is often easy to detect **spoofed** messages
 - sometimes it is hard or almost impossible
- a good chance is to analyze the complete message (full header + body)
 - standard e-mail clients normally hide most of the header, since considered uninteresting
 - the analyst has to get the integral and original message: no standard GUI, IMAP can be good means
 - check fields **From, Return-Path, Reply-To, Received**
 - compare values (not all fields necessarily present in header)
 - lookup IP numbers (if any) and check domain names
 - many tools available for that

SPAM EXAMPLE

- message delivered to official e-mail address, published in web site
- Thunderbird labeled it as spam
- sender looks to be "Mr Jamice Williams"
- delivered to multiple hidden recipients (BCC)
- in Thunderbird (Mac OS) source (full text) of message can be quickly obtained by pressing CMD-U



SPAM ANALYSIS

a few
interesting
headers

Sorgente di: imap://damore@imap.dis.uniroma1.it:993/fetch%3EUID%3E/Junk%3E48069

Return-Path: <mrjamicewilliams@hotmail.com@uictech.com.cn>
X-Original-To: damore@dis.uniroma1.it
Delivered-To: damore@dis.uniroma1.it
Received: from localhost (webmail.dis.uniroma1.it [151.100.59.69])
by mail.dis.uniroma1.it (Postfix) with ESMTP id 9333B22174
for <damore@dis.uniroma1.it>; Sat, 10 Mar 2012 00:47:47 +0100 (CET)
Received: from webmail.dis.uniroma1.it ([127.0.0.1])
by localhost (webmail [127.0.0.1]) (amavisd-new, port 10024) with ESMTP
id 28570-13 for <damore@dis.uniroma1.it>;
Sat, 10 Mar 2012 00:47:42 +0100 (CET)
Received: from mial.uictech.com.cn (unknown [121.52.214.219])
by webmail.dis.uniroma1.it (Postfix) with SMTP id 1BD9026AF0A
for <damore@dis.uniroma1.it>; Sat, 10 Mar 2012 00:47:01 +0100 (CET)
Received: from User ([41.203.64.130])
(envelope-sender <mrjamicewilliams@hotmail.com>)
by 121.52.214.219 with ESMTP
for <damore@dis.uniroma1.it>; Sat, 10 Mar 2012 07:45:31 +0800
Reply-To: <mrjamicewilliams@hotmail.com>
From: "Mr Jamice Williams" <mrjamicewilliams@hotmail.com@dis.uniroma1.it>
Subject: ***SPAM*** TRANSFER OF US\$6,800,000.00 TO YOUR BANK ACCOUNT.
Date: Fri, 9 Mar 2012 15:45:36 -0800
MIME-Version: 1.0
Content-Type: text/html;
charset="Windows-1251"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
X-Antivirus: avast! (VPS 120309-0, 03/09/2012), Outbound message
X-Antivirus-Status: Clean
Message-Id: <20120309234701.1BD9026AF0A@webmail.dis.uniroma1.it>
To: undisclosed-recipients;
X-Virus-Scanned: by amavisd-new at dis.uniroma1.it
X-Spam-Status: Yes, hits=9.2 tagged_above=-99.0 required=8.0 tests=BAYES_50,
FORGED_HOTMAIL_RCVD2, FORGED_MUA_OUTLOOK, FORGED_OUTLOOK_HTML,
FORGED_OUTLOOK_TAGS, HTML_MESSAGE, MIME_HTML_ONLY, MSOE_MID_WRONG_CASE,
RCVD_IN_BL_SPAMCOP_NET, RCVD_IN_SORBS_WEB, RDNS_NONE, SUBJ_ALL_CAPS,
US_DOLLARS_3
X-Spam-Level: *****
X-Spam-Flag: YES

FIRST HOP


questions

- a) whom 41.203.64.130 is registered to?
- b) whom 121.52.214.219 is registered to?
- c) whom euroa-gazette.com.au is registered to?
- d) are these data compatible?

first hop basic data

Received: from User
([41.203.64.130]) (envelope-sender
<mrjamicewilliamshotmail.com>) by
121.52.214.219 with ESMTP for
<damon@euroa-gazette.com.au>; Sat,
10 Mar 2012 07:45:31 +0800

IP Information for 41.203.64.130

IP Location:	 Nigeria Abuja Glo-mobile
ASN:	AS37148
IP Address:	41.203.64.130 W R P D T

inetnum: 41.203.64.0 - 41.203.65.255
netname: GLOBACOM
descr: GLO-Mobile Network Services
country: NG
admin-c: PA2-AFRINIC
tech-c: PA2-AFRINIC
status: ASSIGNED PA
mnt-by: GLO-ONLINE-ADMIN
source: AFRINIC # Filtered
parent: 41.203.64.0 - 41.203.95.255


person: Prasoon Agarwal
nic-hdl: PA2-AFRINIC
address: 1- Mike Adenuga Close, Victoria Island
address: Lagos
address: Lagos
address: Nigeria
e-mail: michael.okoduwa@gloworld.com

phone: +2348055571050
phone: +2348055570601
source: AFRINIC # Filtered

moreover

- euroa-gazette.com.au is registered to "Euroa Gazette Newspaper", an Aussie company
- the website of "The Euroa Gazette" for long time (about 2 years) showed news of October 13, 2009 (message has been sent on March 10, 2012)

IP Information for 121.52.214.219

IP Location:	 China Beijing Beijing Topnew Info&tech Co .ltd
ASN:	AS4808
IP Address:	121.52.214.219 W R P D T
Reverse IP:	2 websites use this address. (examples: tanchengtax.com uictech.com.cn)

inetnum: 121.52.208.0 - 121.52.223.255
netname: TopnewNET
descr: Beijing Topnew Info&Tech co.,LTD.
descr: No.9 A JintailiJiaf~Chaoyang District~Beijing China
country: CN
admin-c: HG335-AP
tech-c: CL1725-AP
mnt-by: MAINT-CNNIC-AP
mnt-lower: MAINT-CNNIC-AP
mnt-routes: MAINT-CNNIC-AP
status: ALLOCATED PORTABLE
changed: hm-changed@apnic.net 20071107
source: APNIC

person: Hongbo Gao
nic-hdl: HG335-AP
e-mail: gao@topnew.cn

address: No.9 A JintailiJiaf~Chaoyang District~Beijing China
phone: +86-10-52081277
fax-no: +86-10-52081280
country: CN
changed: ipas@cnnic.net.cn 20071106
mnt-by: MAINT-CNNIC-AP
source: APNIC

person: Chaocheng Li
nic-hdl: CL1725-AP
e-mail: lcc@topnew.cn

address: No.9 A JintailiJiaf~Chaoyang District~Beijing China
phone: +86-10-52081208
fax-no: +86-10-52081280
country: CN
changed: ipas@cnnic.net.cn 20071106
mnt-by: MAINT-CNNIC-AP
source: APNIC

courtesy of

RESULT OF FIRST-HOP ANALYSIS

message has been **sent** from a host registered to some Nigerian organization and **received** by a Chinese organization, that has been also informed that the **final recipient** belongs to an Aussie organization

SECOND HOP

questions

- a) whom `mial.uictech.com.cn` is registered to?
- b) why IP `121.52.214.219` is labeled as **unknown**?
- c) what compatibility between such data?

second hop basic data

Received: from `mial.uictech.com.cn`
(unknown [121.52.214.219])

by `webmail.dis.uniroma1.it`
(Postfix) with SMTP id 1BD9026AF0A

for
<damore@dis.uniroma1.it>; Sat, 10
Mar 2012 00:47:01 +0100 (CET)

SECOND-HOP ANALYSIS

>whois uictech.com.cn

Domain Name: uictech.com.cn
ROID: 20061205s10011s12255687-cn
Domain Status: ok
Registrant ID: hc812883321-cn
Registrant Organization: 北京联友创嘉科技发展有限公司
Registrant Name: 陈文杰
Registrant Email:
Sponsoring Registrar: 北京万网志成科技有限公司
Name Server: dns11.hichina.com
Name Server: dns12.hichina.com
Registration Date: 2006-12-05 16:32:09
Expiration Date: 2012-12-05 16:32:09
Dnssec Deployment: N

after three attempts (first ones were void):

>nslookup uictech.com.cn

Non-authoritative answer:

Name: uictech.com.cn

Address: 121.52.214.219

**data are
compatible!**

RESULT OF ANALYSIS

- message from Nigeria to China (with claimed final destination in Australia), then from China to Italy looks scarcely convincing
 - in particular there seems to be no reason why the Chinese server has delivered it to server in Sapienza (no explicit recipients of Sapienza are written in message)
- identity of Chinese server appears to be reasonably assured, since it is confirmed by Sapienza server
 - if Sapienza server was been captured, confirmation is unreliable
- initial Nigerian origin is only attested by Chinese server

**MESSAGE IS COMPATIBLE WITH A PHISHING ATTEMPT
ORIGINATED IN CHINA AND DELIVERED WITH SPOOFING
TECHNIQUES AND ADULTERATED HEADERS**