UNIVERSITY INSTITUTE OF ENGINEERING

Department of Computer Science & Engineering

Subject Name: Web And Mobile Security Lab

Subject Code: 20CSP-338

Submitted to: Renuka Ratten

Faculty name: Renuka Ratten

Submitted by: Pranjal Kumar

Name: Pranjal Kumar

UID: 20BCS3504

Section: 607

Group: B

Ex. No	List of Experiments	Conduct (MM: 12)	Viva (MM: 10)	Record (MM: 8)	Total (MM: 30)	Date	Remarks/Signature
1.1	Open any website on computer system and identify http packet on monitoring tool like Wireshark.					19/08/22	
1.2	Design a method to simulate the HTML injections and cross-site scripting (XSS) to exploit the attackers.					28/08/22	
1.3	Implementation of Cross site request forgery (XSRF) attack.					16/09/22	
1.4	Implementation of Design methods to break authentication schemes (SQL Injection attack).					04/10/22	
2.1	Write a program to generate message digest for the given message using the SHA/MD5 algorithm and verify the integrity of message.					19/10/22	
2.2	Perform Penetration testing on a web application to gather information about the system (Foot Printing).					03/11/22	

Experiment 2.2

Student Name: Pranjal Kumar	**UID: 20BS3504**
Branch: CSE	**Section/Group: 607-B**
Semester: 5th	**Date of Performance: 03/11/22**
Subject Name: WMS Lab	**Subject Code: CSP-338**

AIM:

Perform Penetration testing on a web application to gather Information about the system (Foot Printing).

REQUIREMENTS:

- Windows 10
- Good Internet Connectivity

TOOLS TO BE USED:

- Ht-Track
- Any Demo website
- Active G-mail Account
- Whois IP Lookup website

THEORY:

Foot-printing means gathering information about a target system that can be used to execute a successful cyber-attack. To get this information, a hacker might use various methods with variant tools. This information is the first road for the hacker to crack a system.

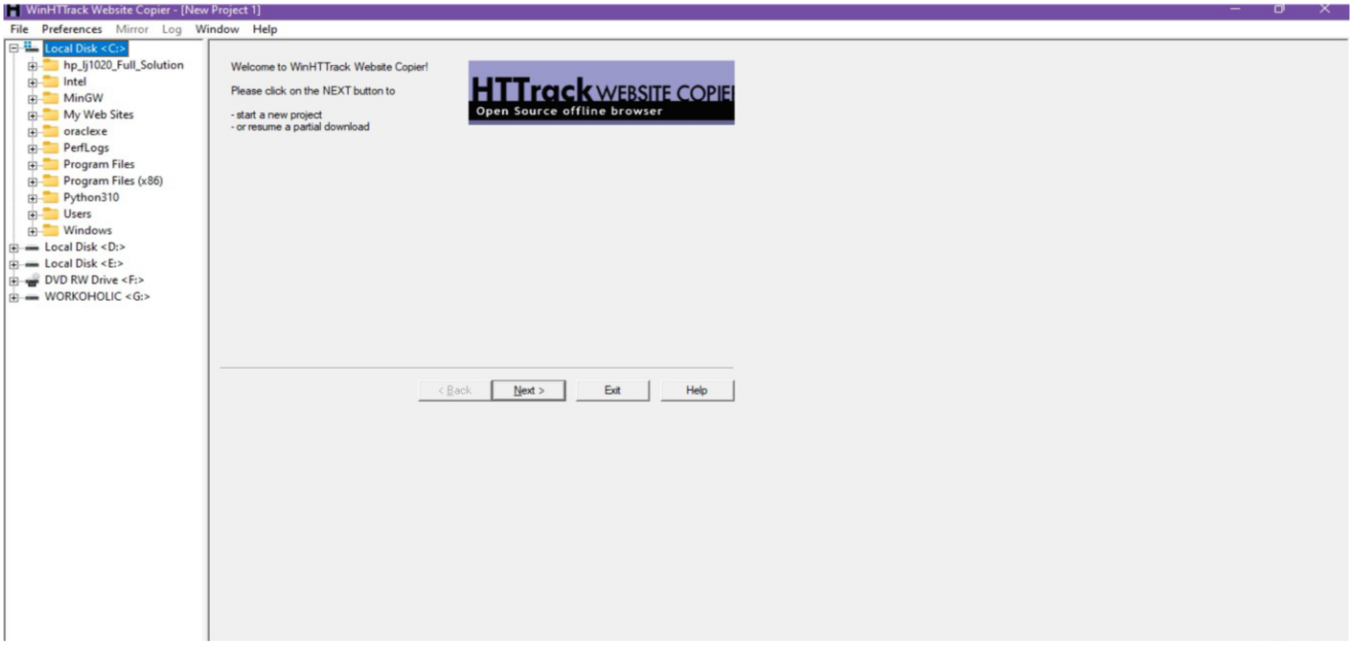
Different kinds of information that can be gathered from Footprinting are as follows:

1. The operating system of the target machine
2. Firewall
3. IP address
4. Network map
5. Security configurations of the target machine
6. Email id, password
7. Server configurations
8. URLs

STEPS and SNAPSHOTS:

WEBSITE FOOT-PRINTING (MIRRORING OF WEBSITE)

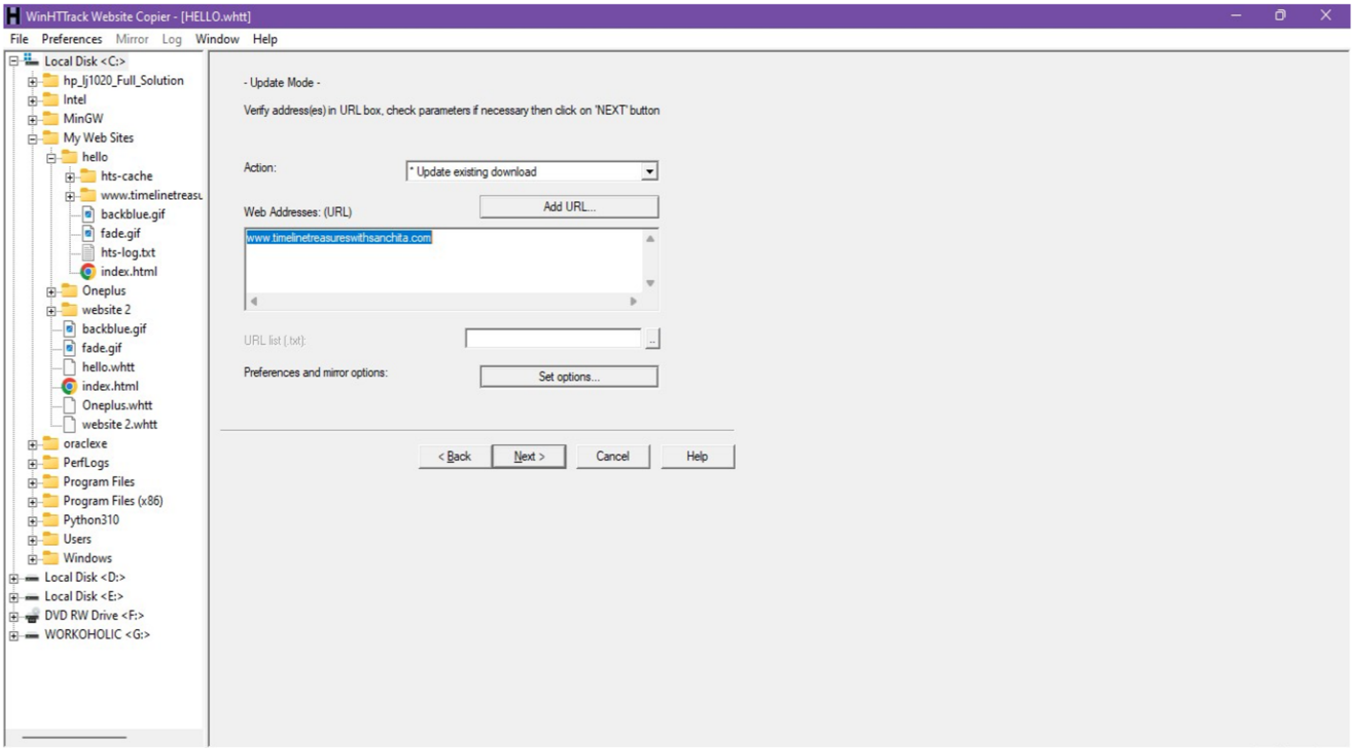
1. Go to Google and open Ht-Track link and download first link.
2. Install this tool and put URL of any demo website to copy the website.
3. To check the detail coding and web pages of copied website just go to the location where this tool is installed i.e. C-drive.



Welcome to WinHTTrack Website Copier!

Please click on the NEXT button to

- start a new project
- or resume a partial download



- Update Mode -

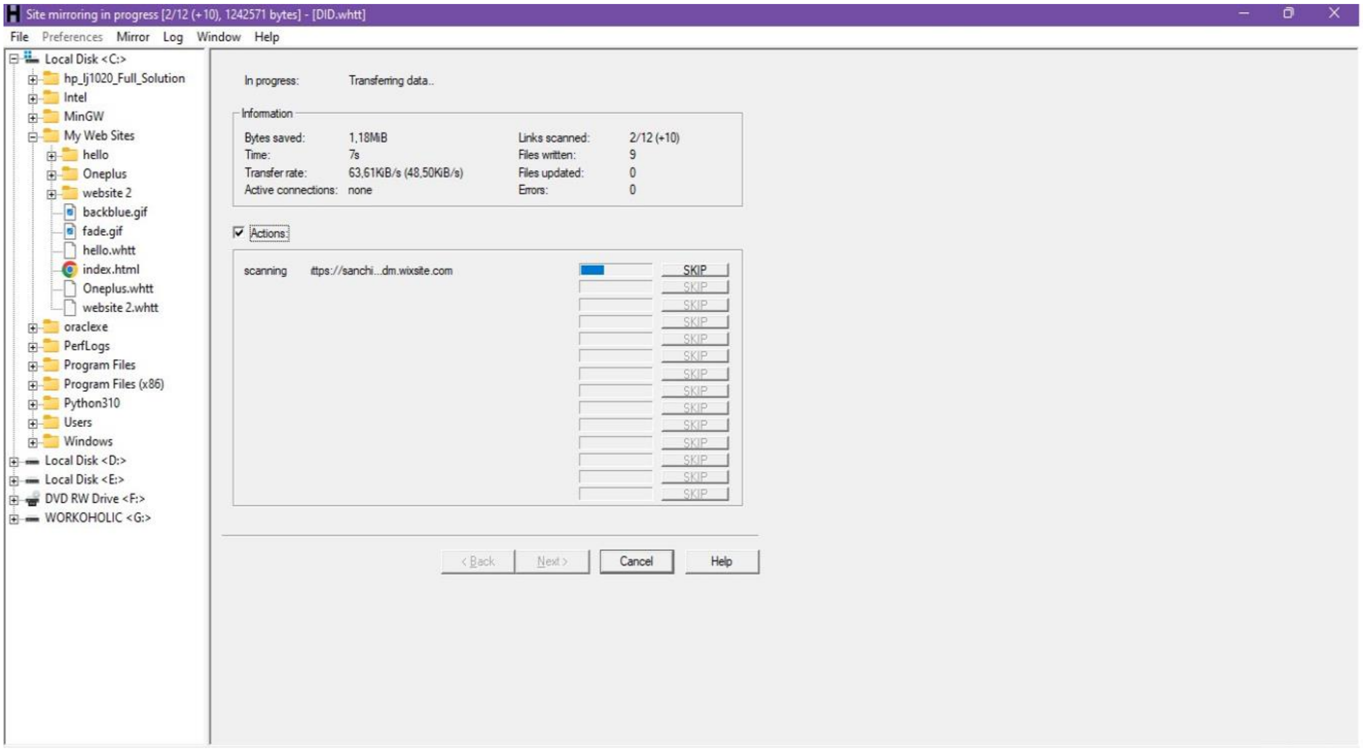
Verify address(es) in URL box, check parameters if necessary then click on 'NEXT' button

Action: * Update existing download

Web Addresses: (URL) www.timelinetreasureswithsanchita.com

URL list (.txt):

Preferences and mirror options:



Site mirroring in progress [2/12 (+10), 1242571 bytes] - [DID.whtt]

In progress: Transferring data..

Information

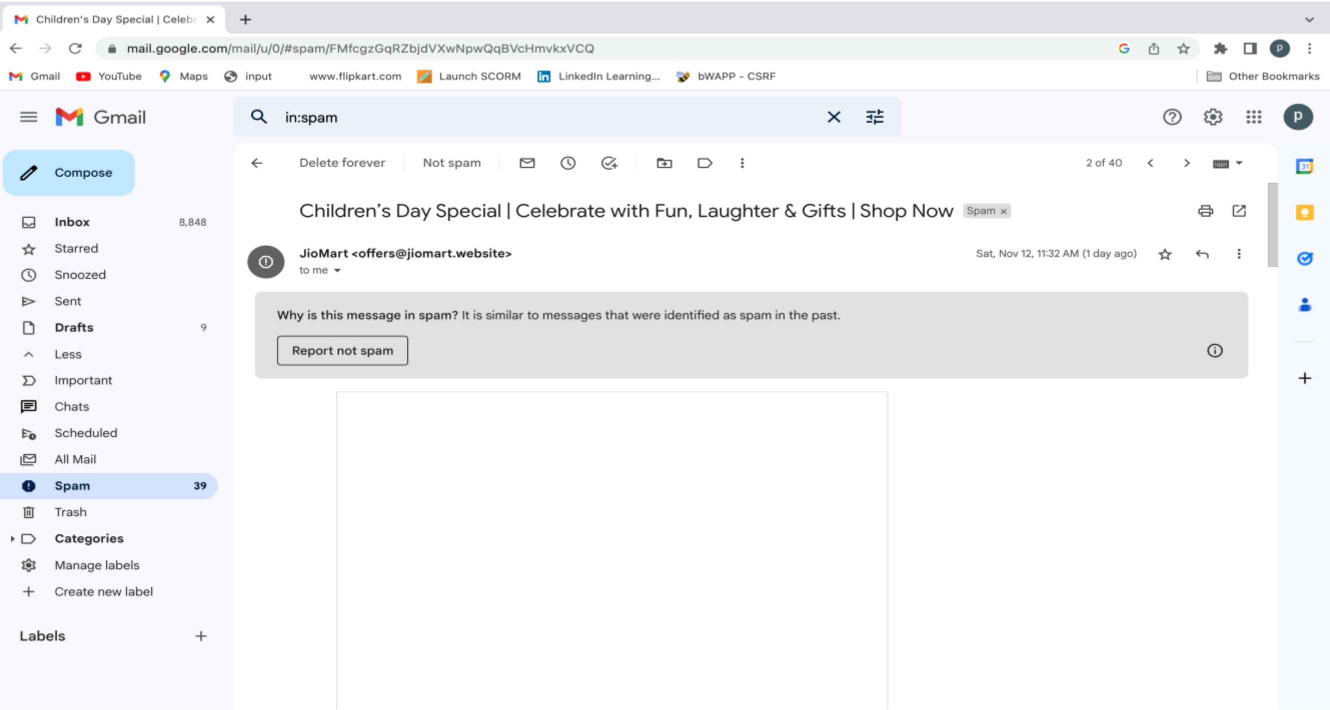
Bytes saved: 1,18MiB
Time: 7s
Transfer rate: 63,61KiB/s (48,50KiB/s)
Active connections: none
Links scanned: 2/12 (+10)
Files written: 9
Files updated: 0
Errors: 0

☑ Actions:

scanning ttps://sanchi...dm.wixsite.com

E-MAIL FOOT-PRINTING

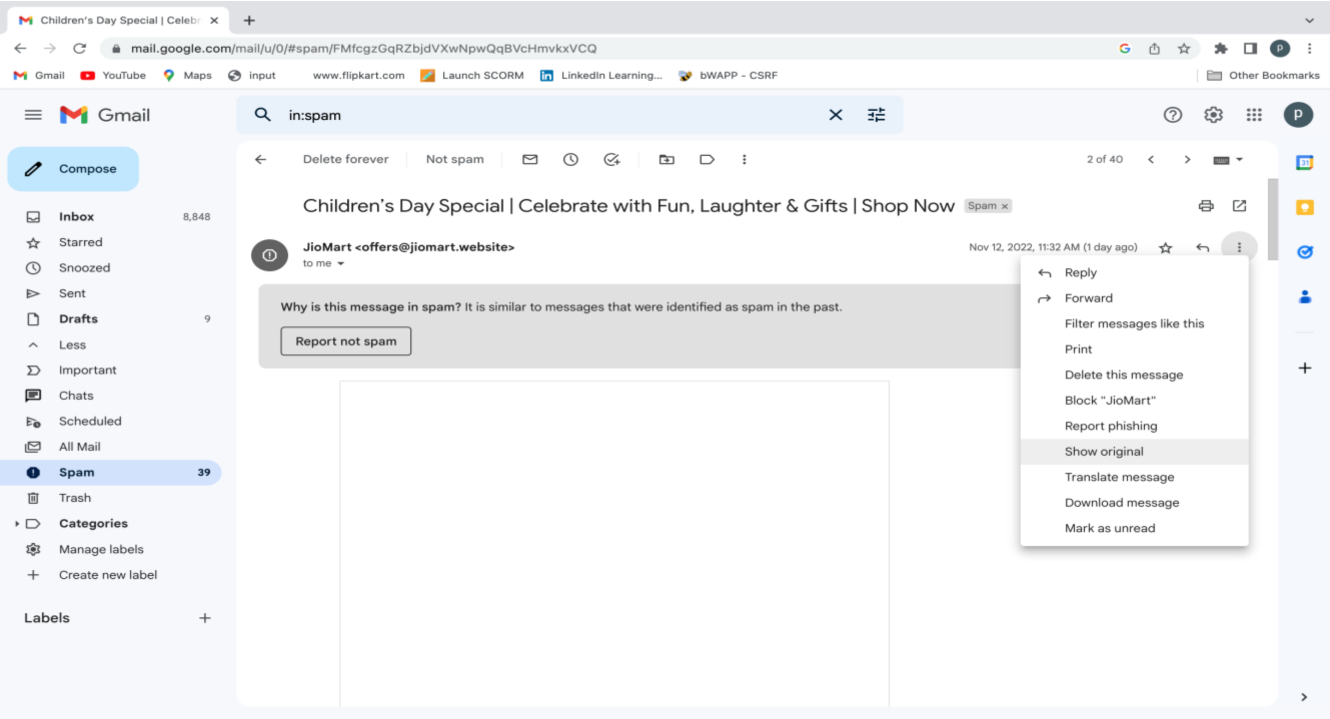
1. Open any spam mail
2. Click on three-dots and click on show original. Search “received from” on page and copy IP Address
3. Open a website ultratools.com or Whois Ip Lookup and paste IPAddress there.
4. You can track all information there.



Children's Day Special | Celebrate with Fun, Laughter & Gifts | Shop Now Spam ×

JioMart <offers@jiomart.website>
to me
Sat, Nov 12, 11:32 AM (1 day ago)

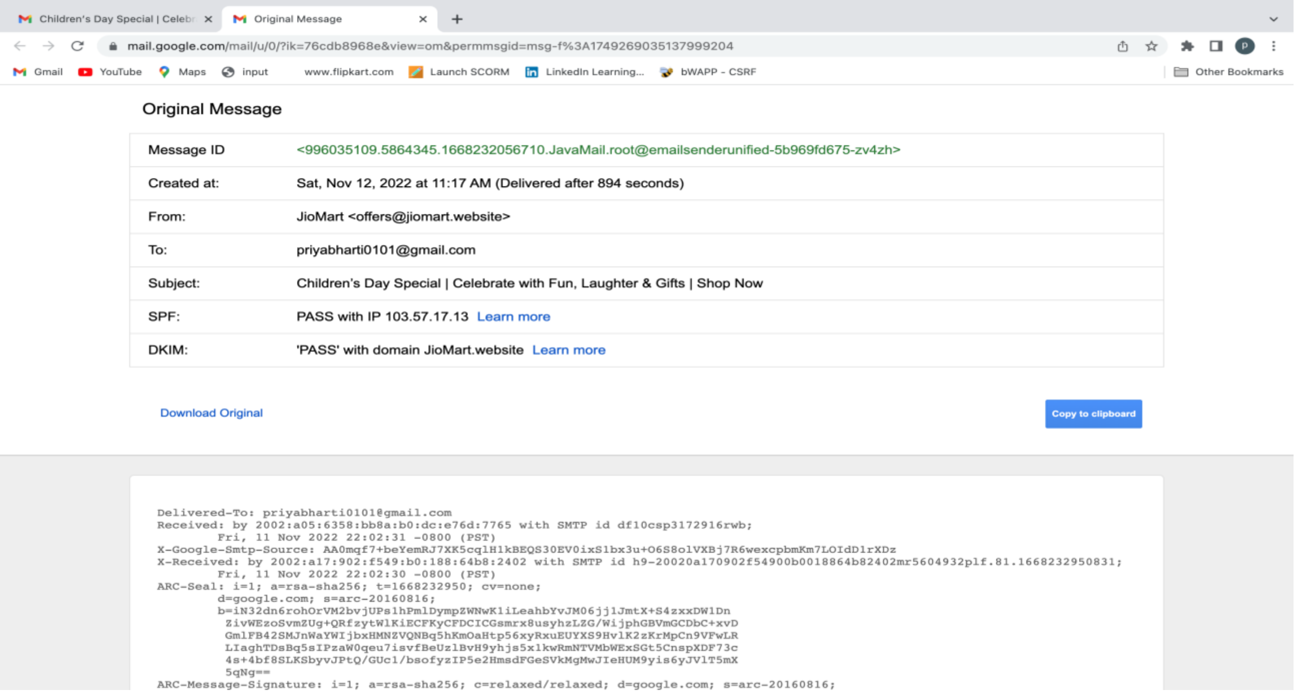
Why is this message in spam? It is similar to messages that were identified as spam in the past.



Children's Day Special | Celebrate with Fun, Laughter & Gifts | Shop Now Spam ×

JioMart <offers@jiomart.website>
to me
Nov 12, 2022, 11:32 AM (1 day ago)

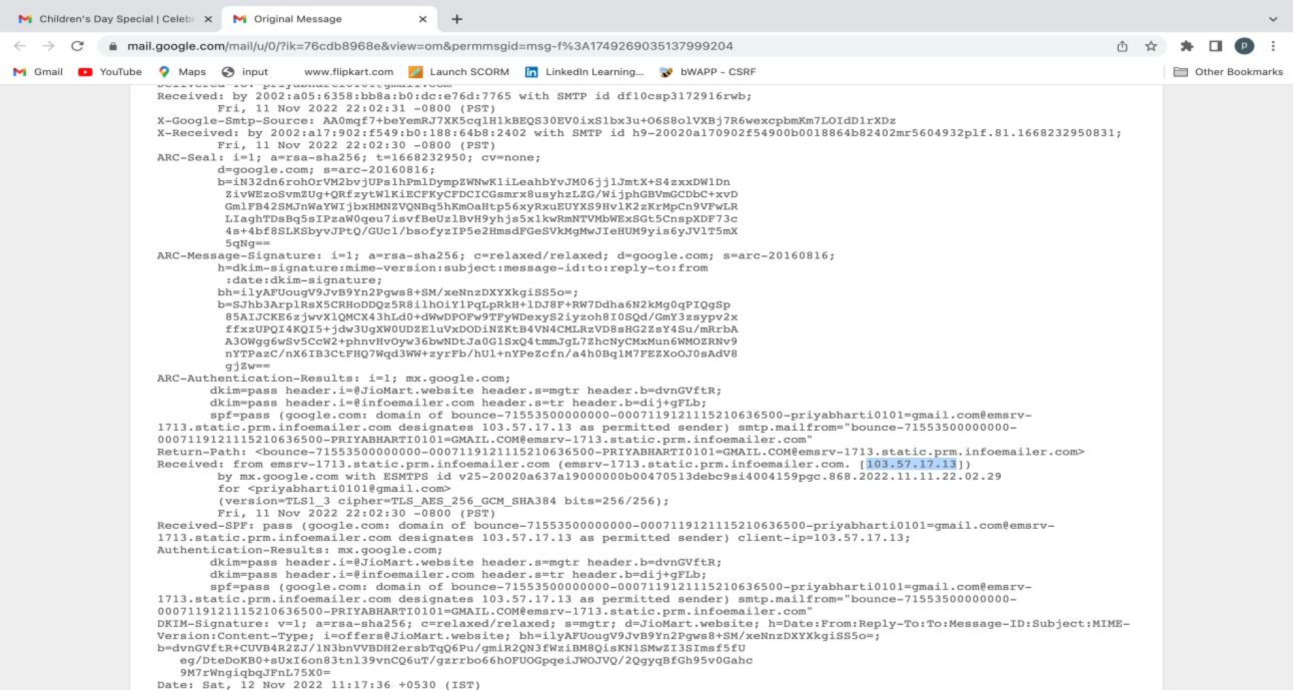
Why is this message in spam? It is similar to messages that were identified as spam in the past.



Original Message

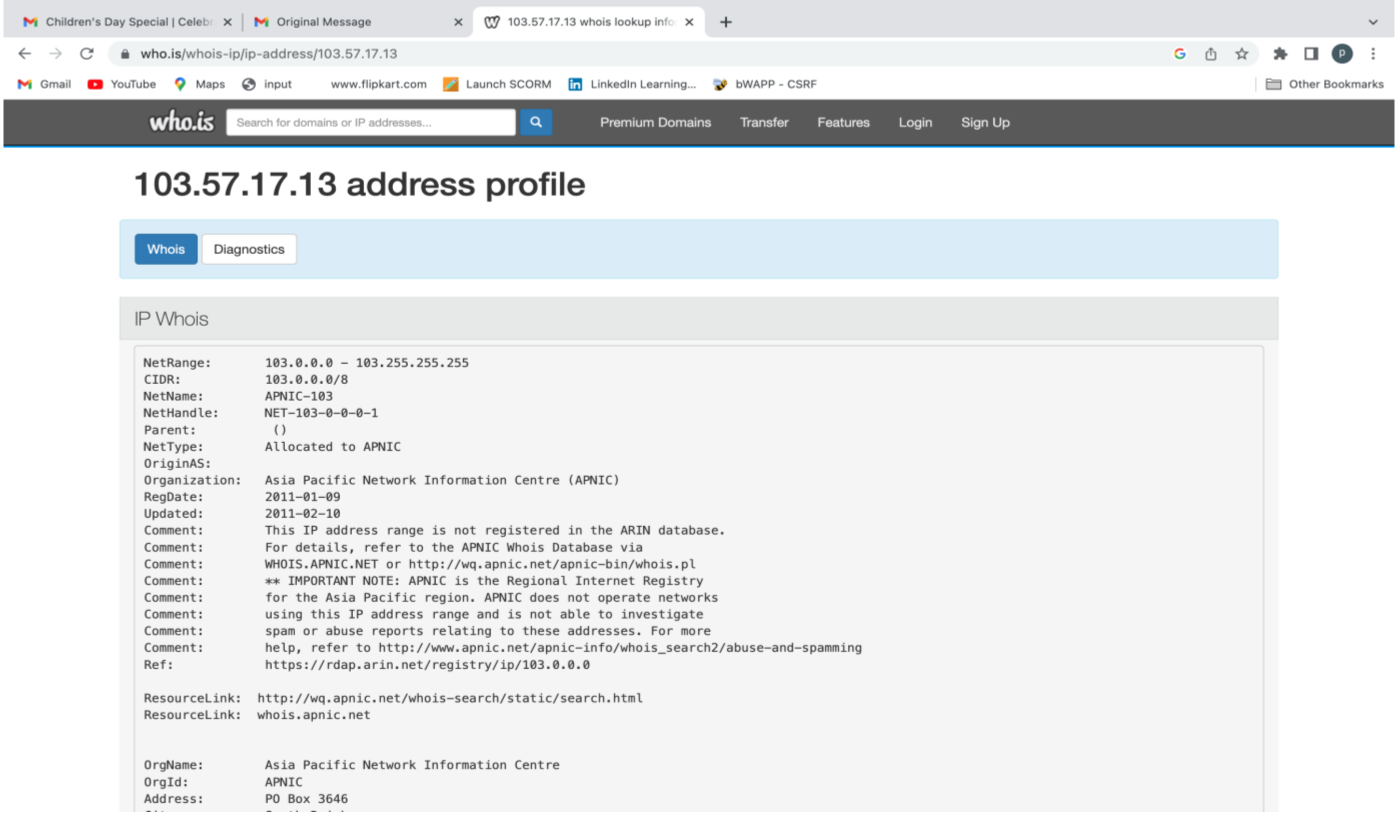
Message ID	<996035109.5864345.1668232056710.JavaMail.root@emailsenderunified-5b969fd675-zv4zh>
Created at:	Sat, Nov 12, 2022 at 11:17 AM (Delivered after 894 seconds)
From:	JioMart <offers@jiomart.website>
To:	priyabharti0101@gmail.com
Subject:	Children's Day Special | Celebrate with Fun, Laughter & Gifts | Shop Now
SPF:	PASS with IP 103.57.17.13 Learn more
DKIM:	'PASS' with domain JioMart.website Learn more

```
Delivered-To: priyabharti0101@gmail.com
Received: by 2002:a05:6358:bb8a:b0:dc:e76d:7765 with SMTP id df10csp3172916rwb;
        Fri, 11 Nov 2022 22:02:31 -0800 (PST)
X-Google-Smtp-Source: AA0mqf7+beYemRJ7XK5cqlH1kBEQS30EV0ixSlbx3u+O6S8olVXBj7R6wexcpbmKm7LOIdD1rXDz
X-Received: by 2002:a17:902:f549:b0:188:64b8:2402 with SMTP id h9-20020a170902f54900b0018864b82402mr5604932plf.81.1668232950831;
        Fri, 11 Nov 2022 22:02:30 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1668232950; cv=none;
        d=google.com; s=arc-20160816;
        b=iN32dn6rohOrVM2bvjUPs1hPmlDympZWNwK1iLeahbYvJM06jj1JmtX+S4zxxDW1Dn
         ZivWEzoSvmZUg+QRfzytWlKiECFKyCFDCICGsmrx8usyhzLZG/WijphGBVmGCDbC+xvD
         GmlFB42SMJnWaYWIjbxHMNZVQNBq5hKmOaHtp56xyRxuEUYXS9HvlK2zKrMpCn9VFwLR
         LIaghTDsBq5sIPzaW0qeu7isvfBeUzlBvH9yhjs5x1kwRmNTVMbWExSGt5CnspXDF73c
         4s+4bf8SLKSbyvJPtQ/GUc1/bsofyzIP5e2HmsdFGeSVkMgMwJIeHUM9yis6yJVlT5mX
         5qNg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
```


Children's Day Special | Celebr
Original Message
mail.google.com/mail/u/0/?ik=76cdb8968e&view=om&permmsgid=msg-f%3A1749269035137999204
Gmail
YouTube
Maps
input
www.flipkart.com
Launch SCORM
LinkedIn Learning...
bWAPP - CSRF
Other Bookmarks

```
Received: by 2002:a05:6358:bb8a:b0:dc:e76d:7765 with SMTP id df10csp3172916rwb;
        Fri, 11 Nov 2022 22:02:31 -0800 (PST)
X-Google-Smtp-Source: AA0mqf7+beYemRJ7XK5cqlH1kBEQS30EV0ixSlbx3u+O6S8olVXBj7R6wexcpbmKm7LOIdD1rXDz
X-Received: by 2002:a17:902:f549:b0:188:64b8:2402 with SMTP id h9-20020a170902f54900b0018864b82402mr5604932plf.81.1668232950831;
        Fri, 11 Nov 2022 22:02:30 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1668232950; cv=none;
        d=google.com; s=arc-20160816;
        b=iN32dn6rohOrVM2bvjUPs1hPmlDympZWNwK1iLeahbYvJM06jj1JmtX+S4zxxDW1Dn
         ZivWEzoSvmZUg+QRfzytWlKiECFKyCFDCICGsmrx8usyhzLZG/WijphGBVmGCDbC+xvD
         GmlFB42SMJnWaYWIjbxHMNZVQNBq5hKmOaHtp56xyRxuEUYXS9HvlK2zKrMpCn9VFwLR
         LIaghTDsBq5sIPzaW0qeu7isvfBeUzlBvH9yhjs5x1kwRmNTVMbWExSGt5CnspXDF73c
         4s+4bf8SLKSbyvJPtQ/GUc1/bsofyzIP5e2HmsdFGeSVkMgMwJIeHUM9yis6yJVlT5mX
         5qNg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
```

```
        h=dkim-signature:mime-version:subject:message-id:to:reply-to:from
         :date:dkim-signature;
        bh=ilyAFUougV9JvB9Yn2Pgws8+SM/xeNnzDXYXkgiSS5o=;
        b=SJhb3ArplRsX5CRHoDDQz5R8ilhOiY1PqLpRkH+lDJ8F+RW7Ddha6N2kMg0qPIQgSp
         85AIJCKE6zjwvXlQMCX43hLd0+dWwDPOFw9TFyWDexyS2iyzoh8I0SQd/GmY3zsypv2x
         ffxzUPQI4KQI5+jdw3UgXW0UDZEluVxDODiNZKtB4VN4CMLRzVD8sHG2ZsY4Su/mRrbA
         A3OWgg6wSv5CcW2+phnvHvOyw36bwNDtJa0G1SxQ4tmmJgL7ZhcNyCMxMun6WMOZRNv9
         nYTPazC/nX6IB3CtFHQ7Wqd3WW+zyrFb/hUl+nYPeZcfn/a4h0Bq1M7FEZXoOJ0sAdV8
         gjZw==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@JioMart.website header.s=mgtr header.b=dvnGVftR;
       dkim=pass header.i=@infoemailer.com header.s=tr header.b=dij+gFLb;
       spf=pass (google.com: domain of bounce-71553500000000-007119121115210636500-priyabharti0101=gmail.com@emsrv-
1713.static.prm.infoemailer.com designates 103.57.17.13 as permitted sender) smtp.mailfrom="bounce-71553500000000-
007119121115210636500-PRIYABHARTI0101=GMAIL.COM@emsrv-1713.static.prm.infoemailer.com"
Return-Path: <bounce-71553500000000-007119121115210636500-PRIYABHARTI0101=GMAIL.COM@emsrv-1713.static.prm.infoemailer.com>
Received: from emsrv-1713.static.prm.infoemailer.com (emsrv-1713.static.prm.infoemailer.com. [103.57.17.13])
        by mx.google.com with ESMTPS id v25-20020a637a19000000b00470513debc9si4004159pgc.868.2022.11.11.22.02.29
        for <priyabharti0101@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Fri, 11 Nov 2022 22:02:30 -0800 (PST)
Received-SPF: pass (google.com: domain of bounce-71553500000000-007119121115210636500-priyabharti0101=gmail.com@emsrv-
1713.static.prm.infoemailer.com designates 103.57.17.13 as permitted sender) client-ip=103.57.17.13;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@JioMart.website header.s=mgtr header.b=dvnGVftR;
       dkim=pass header.i=@infoemailer.com header.s=tr header.b=dij+gFLb;
       spf=pass (google.com: domain of bounce-71553500000000-007119121115210636500-priyabharti0101=gmail.com@emsrv-
1713.static.prm.infoemailer.com designates 103.57.17.13 as permitted sender) smtp.mailfrom="bounce-71553500000000-
007119121115210636500-PRIYABHARTI0101=GMAIL.COM@emsrv-1713.static.prm.infoemailer.com"
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=mgtr; d=JioMart.website; h=Date:From:Reply-To:To:Message-ID:Subject:MIME-
Version:Content-Type; i=offers@JioMart.website; bh=ilyAFUougV9JvB9Yn2Pgws8+SM/xeNnzDXYXkgiSS5o=;
b=dvnGVftR+CUVB4R2ZJ/1N3bnVVBDH2ersbTqQ6Pu/gmiR2QN3fWziBM8QisKN1SMwZI3SImsf5fU
   eg/DteDoKB0+sUxI6on83tnl39vnCQ6uT/gzrrbo66hOFUOGpqeiJWOJVQ/2QgyqBfGh95v0Gahc
   9M7rWngiqbqJFnL75X0=
Date: Sat, 12 Nov 2022 11:17:36 +0530 (IST)
```



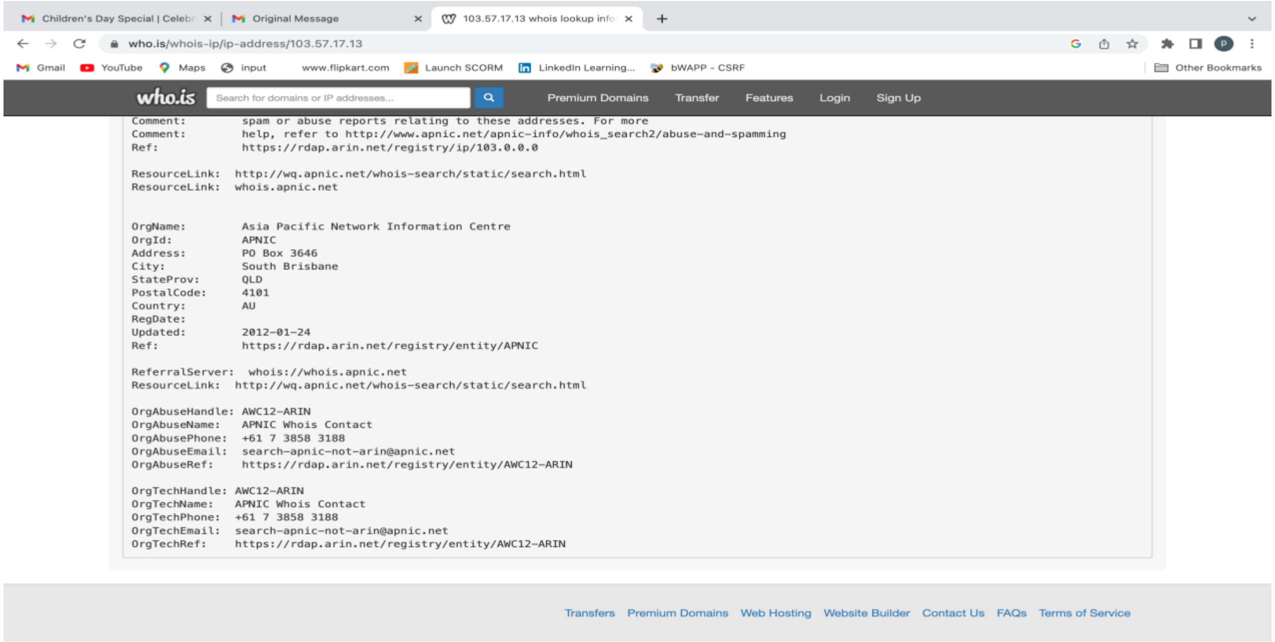
103.57.17.13 address profile

IP Whois

```
NetRange:       103.0.0.0 - 103.255.255.255
CIDR:           103.0.0.0/8
NetName:        APNIC-103
NetHandle:      NET-103-0-0-0-1
Parent:          ()
NetType:        Allocated to APNIC
OriginAS:
Organization:   Asia Pacific Network Information Centre (APNIC)
RegDate:        2011-01-09
Updated:        2011-02-10
Comment:        This IP address range is not registered in the ARIN database.
Comment:        For details, refer to the APNIC Whois Database via
Comment:        WHOIS.APNIC.NET or http://wq.apnic.net/apnic-bin/whois.pl
Comment:        ** IMPORTANT NOTE: APNIC is the Regional Internet Registry
Comment:        for the Asia Pacific region. APNIC does not operate networks
Comment:        using this IP address range and is not able to investigate
Comment:        spam or abuse reports relating to these addresses. For more
Comment:        help, refer to http://www.apnic.net/apnic-info/whois_search2/abuse-and-spamming
Ref:            https://rdap.arin.net/registry/ip/103.0.0.0

ResourceLink:  http://wq.apnic.net/whois-search/static/search.html
ResourceLink:  whois.apnic.net


OrgName:        Asia Pacific Network Information Centre
OrgId:          APNIC
Address:        PO Box 3646
```



```
Comment:        spam or abuse reports relating to these addresses. For more
Comment:        help, refer to http://www.apnic.net/apnic-info/whois_search2/abuse-and-spamming
Ref:            https://rdap.arin.net/registry/ip/103.0.0.0

ResourceLink:  http://wq.apnic.net/whois-search/static/search.html
ResourceLink:  whois.apnic.net


OrgName:        Asia Pacific Network Information Centre
OrgId:          APNIC
Address:        PO Box 3646
City:           South Brisbane
StateProv:      QLD
PostalCode:     4101
Country:        AU
RegDate:
Updated:        2012-01-24
Ref:            https://rdap.arin.net/registry/entity/APNIC

ReferralServer:  whois://whois.apnic.net
ResourceLink:  http://wq.apnic.net/whois-search/static/search.html

OrgAbuseHandle: AWC12-ARIN
OrgAbuseName:   APNIC Whois Contact
OrgAbusePhone:  +61 7 3858 3188
OrgAbuseEmail:  search-apnic-not-arin@apnic.net
OrgAbuseRef:    https://rdap.arin.net/registry/entity/AWC12-ARIN

OrgTechHandle: AWC12-ARIN
OrgTechName:   APNIC Whois Contact
OrgTechPhone:  +61 7 3858 3188
OrgTechEmail:  search-apnic-not-arin@apnic.net
OrgTechRef:    https://rdap.arin.net/registry/entity/AWC12-ARIN
```

LEARNING OUTCOMES:

Finally, as a penetration tester, you should collect and log all vulnerabilities in the system. Don't ignore any scenario considering that it won't be executed by the end-users. If you are a penetration tester, please help our readers with your experience, tips, and sample test cases on how to perform Penetration Testing effectively.

Evaluation Grid :

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.	Student Performance (Conduct of experiment) objectives/Outcomes.		12
2.	Viva Voce		10
3.	Submission of Work Sheet (Record)		8
	Total		30