EMAIL FORENSICS

AND TOOLS FOR THREAT INTELLIGENCE

ERIC NII SOWAH BADGER (NIIHACK)

NiiHack
The Hack Master

Table of Content

Who AM I

- ERIC NII SOWAH BADGER (NiiHack)
- S.O.C. Specialist (Pentest) at GCB Bank Ltd
- CSDS Fellow, Cyberspace
- Content Creator @ Learn with Niihack (LWN)
- YouTube Channel: Learn with Niihack (LWN)
- LinkedIn: Eric Nii Sowah Badger
- TWITTER: ens_nii
- Personal Website: https://www.niihackgh.com
- I play Basketball, Drums and Guitar

NiiHack
The Hack Master

Common Terminologies Associated With Email

SMTP Server

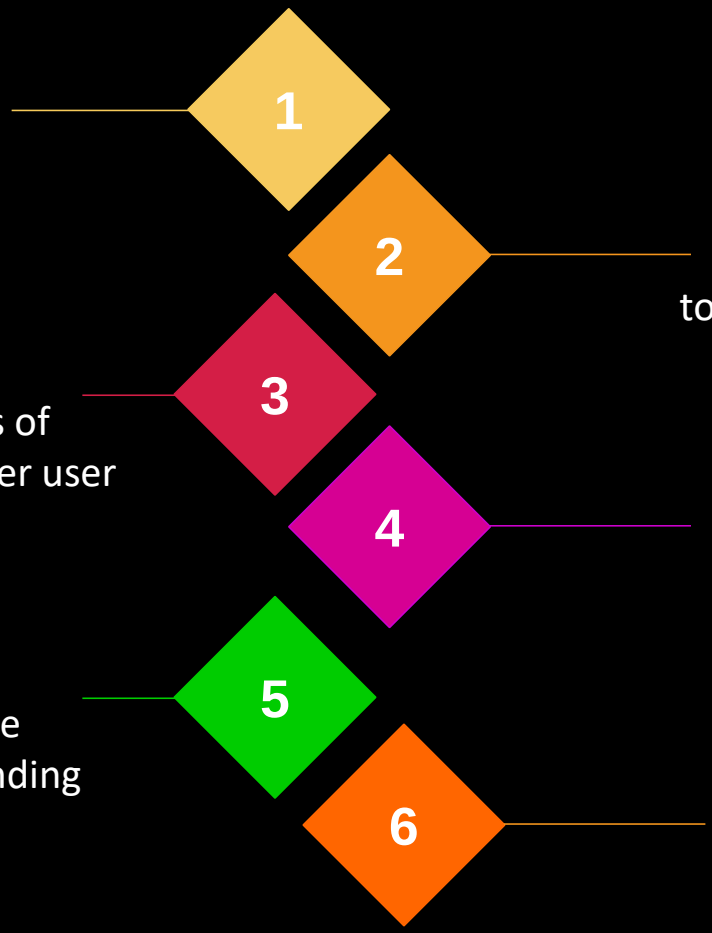
Stands for Simple Mail Transfer Protocol This is an internet standard communication protocol for electronic mail transmission

IMAP Server

Stands for Internet Message Access Protocol Incoming mail Server exhibits same functionality as of POP based server but retain copy of email even after user downloads the email.

DKIM

Stands for DomainKeys Identified Mail
is an email security standard designed to make sure messages aren't altered in transit between the sending and recipient servers.



POP3 Server

Stands for **Post Office Protocol.** It is an incoming mail server that helps the user to RECEIVE the email residing in its e-mailbox..

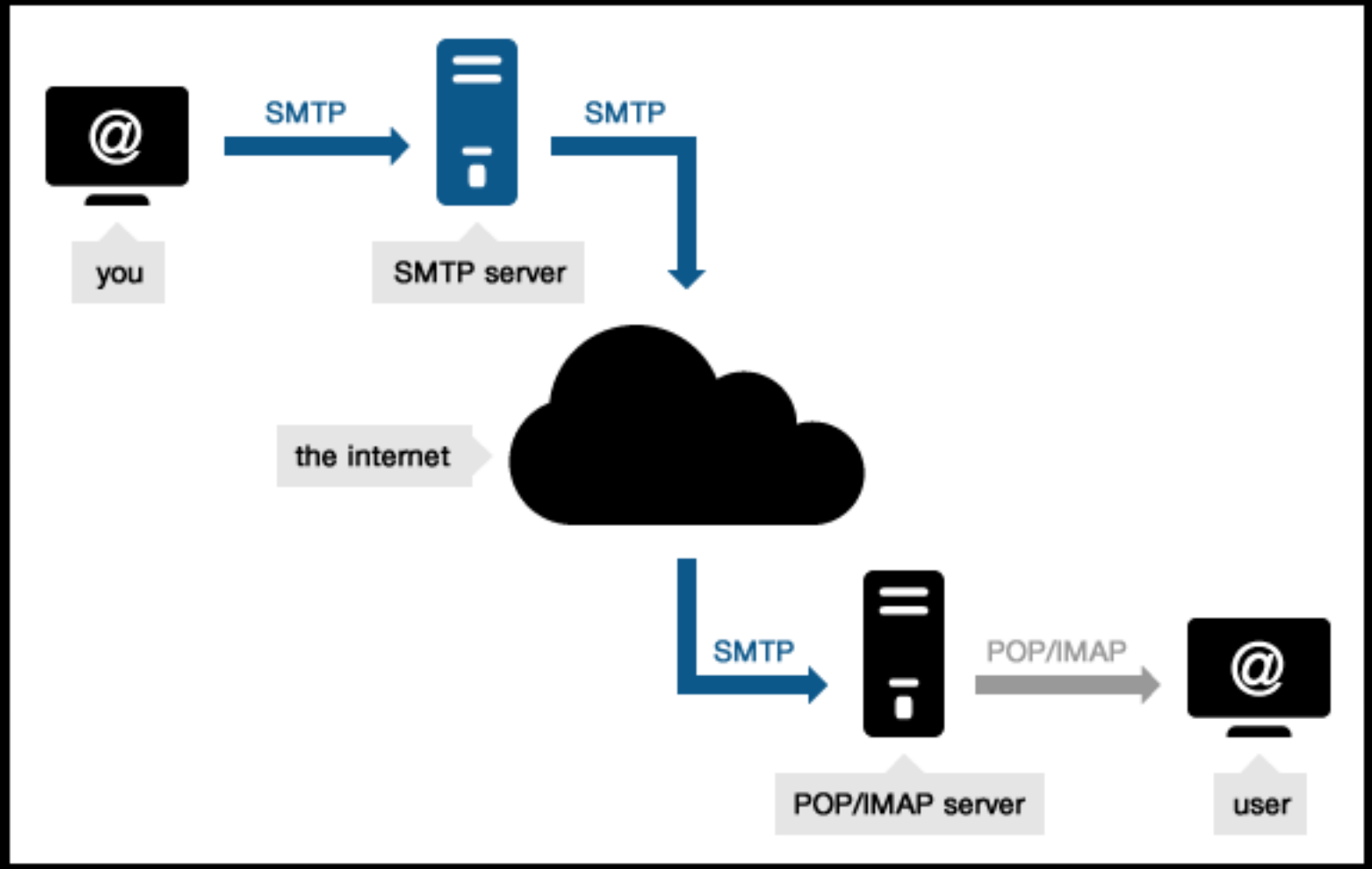
SPF Record

Stands for **Sender Policy Framework.** It is an email authentication standard that helps protect senders and recipients from spam, spoofing, and phishing.

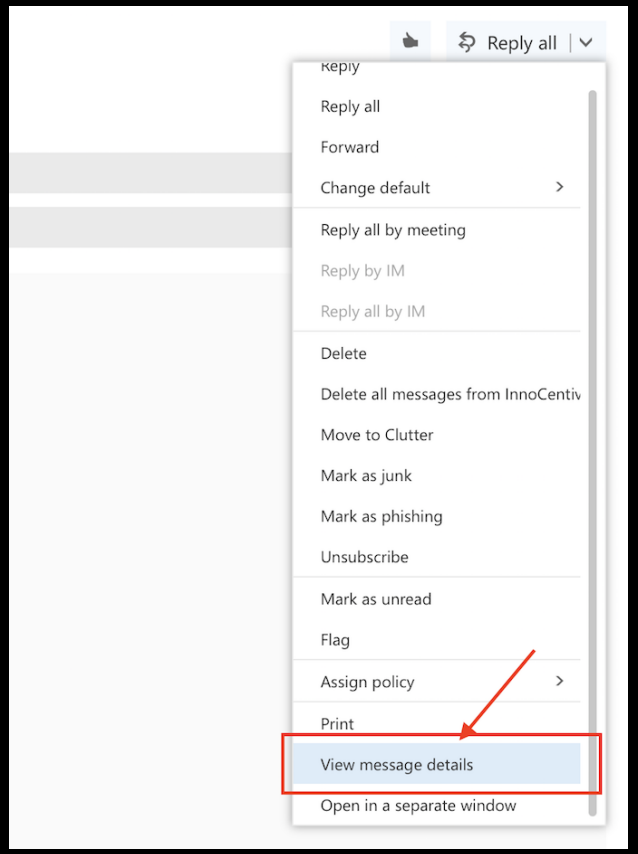
DMARC

Stands for Domain-based Message Authentication, Reporting & Conformance. It is an email authentication, policy, and reporting protocol.

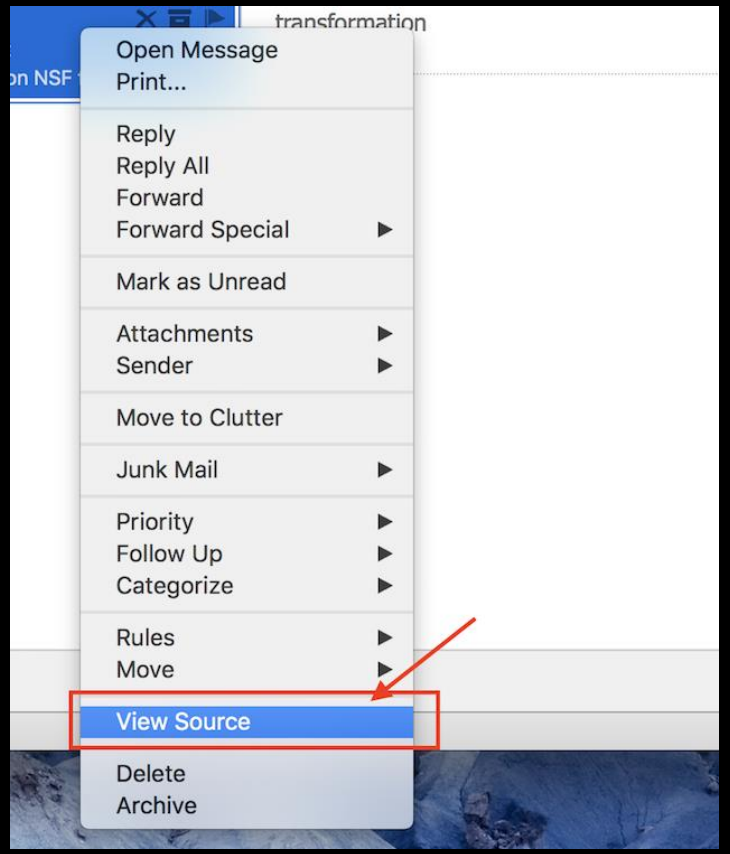
Email Sender to Reciever Path



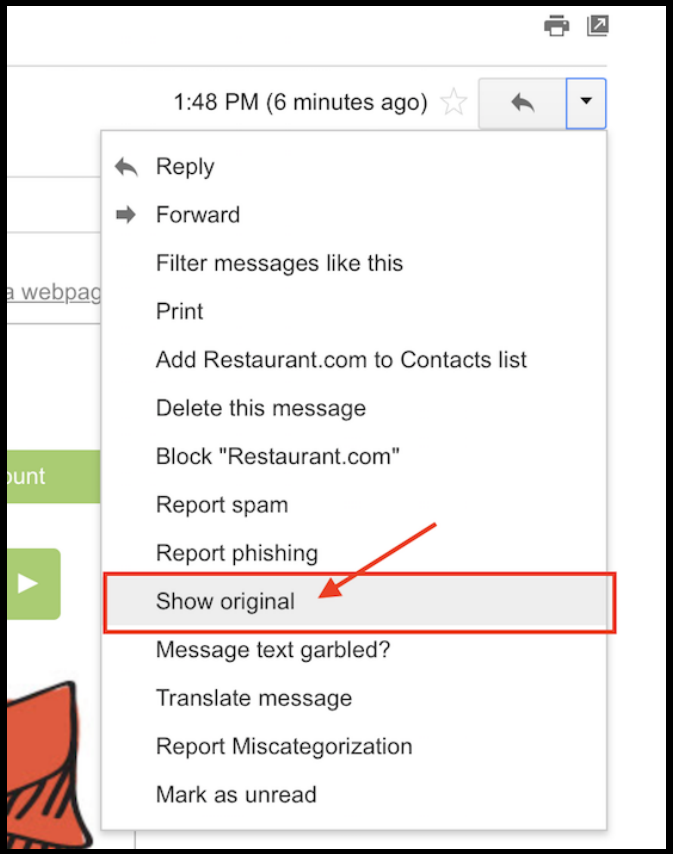
Aquiring Email Headers



- Outlook Web Client



- Outlook Desktop Client

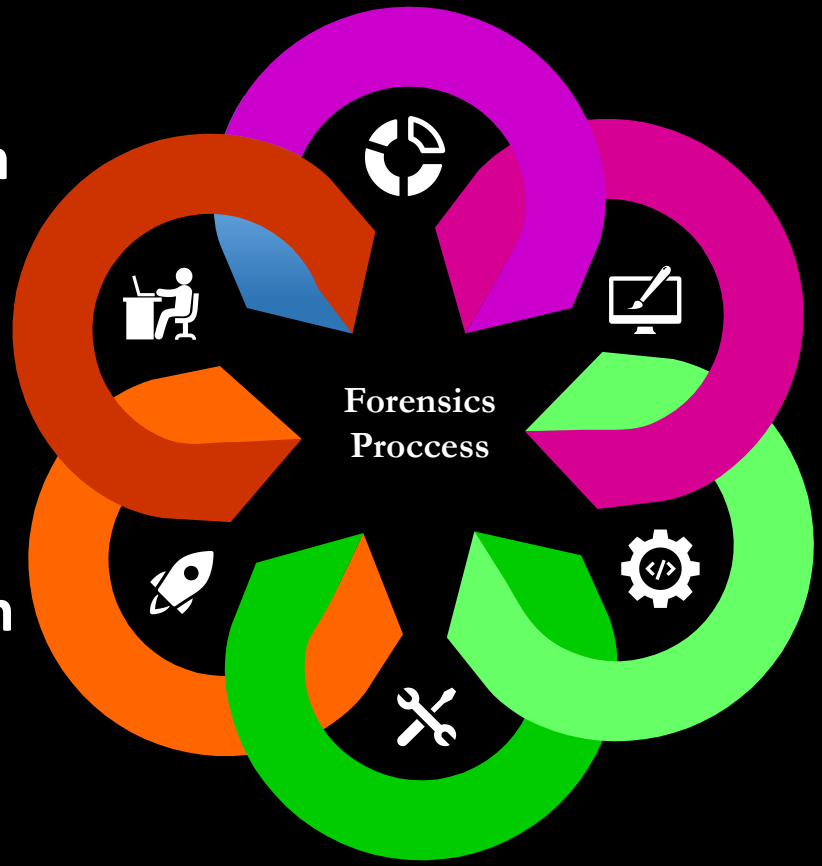


- Gmail

Important Informations in the Email Header

Sender of the email

Encoding information



Network path it traversed and path of origination

Email Client information

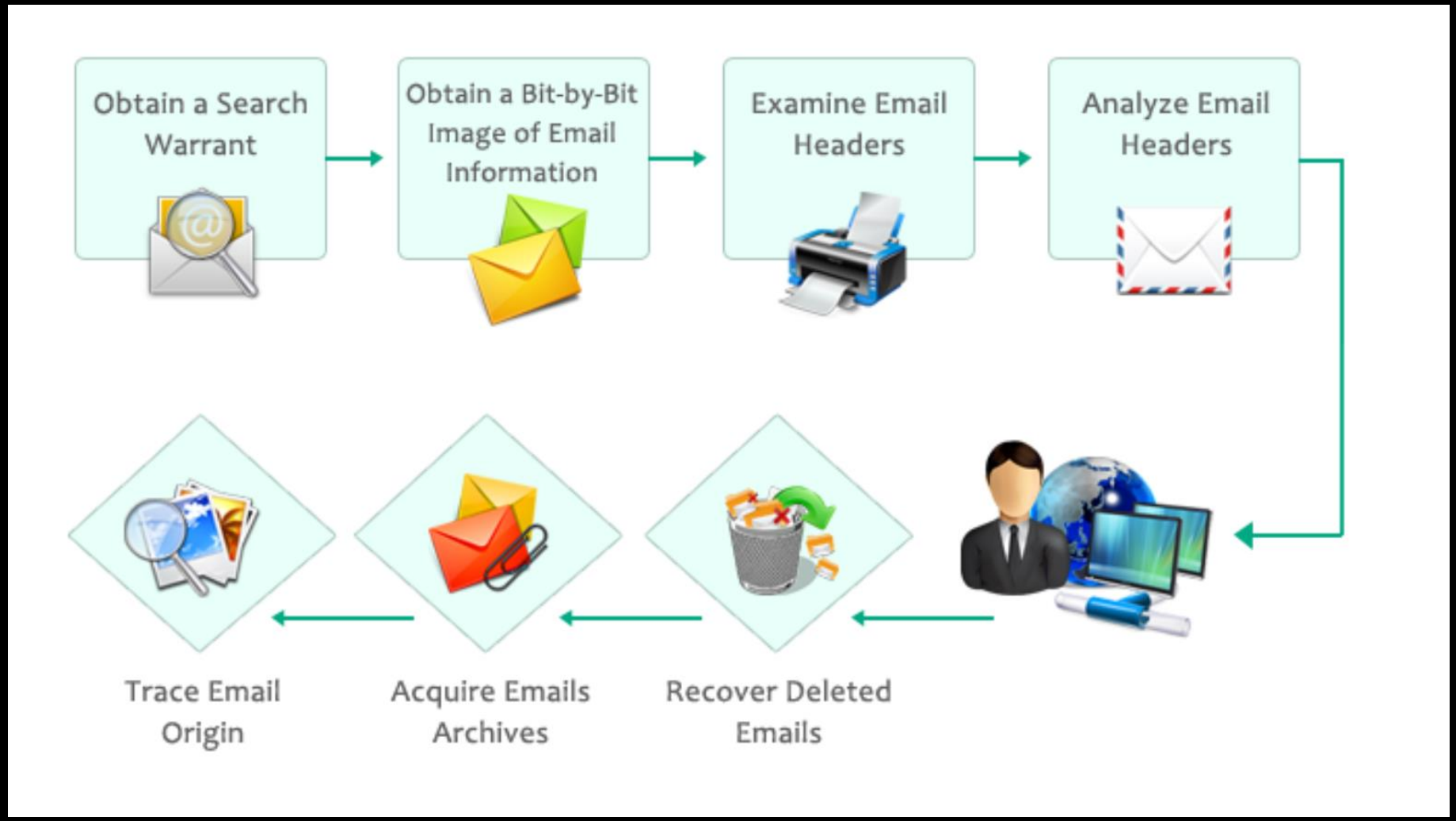
SMTP Servers it went through

Time Stamp Detail

Email Header Forensics

PRACTICALS USING PHISHTOOL

Step in Email Forensics for Investigator



Crimes Committed via Email

Open Source Tools for Threat Intelligence

- Spiderfoot
- TheHavester (https://github.com/laramies/theHarvester)
- Hunter (hunter.io)
- Wappalyser
- Google dorks
- Sublist3r (https://github.com/aboul3la/Sublist3r)
- Assetfinder

NiiHack
The Hack Master

References

- Email Forensics Guide For Beginners – Attack & Preventive Measures (freeviewer.org)
- Phishing - Email Header Analysis · nebraska-gencyber-modules (mlhale.github.io)

Questions

Thank You

TEL/WHATSAPP: 0242004431 **EMAIL: niihack.gh@gmail.com** **WEBSITE: https://www.niihackgh.com**