CYBERSECURITY AND DIGITAL FORENSICS TRAINING WORKSHOP

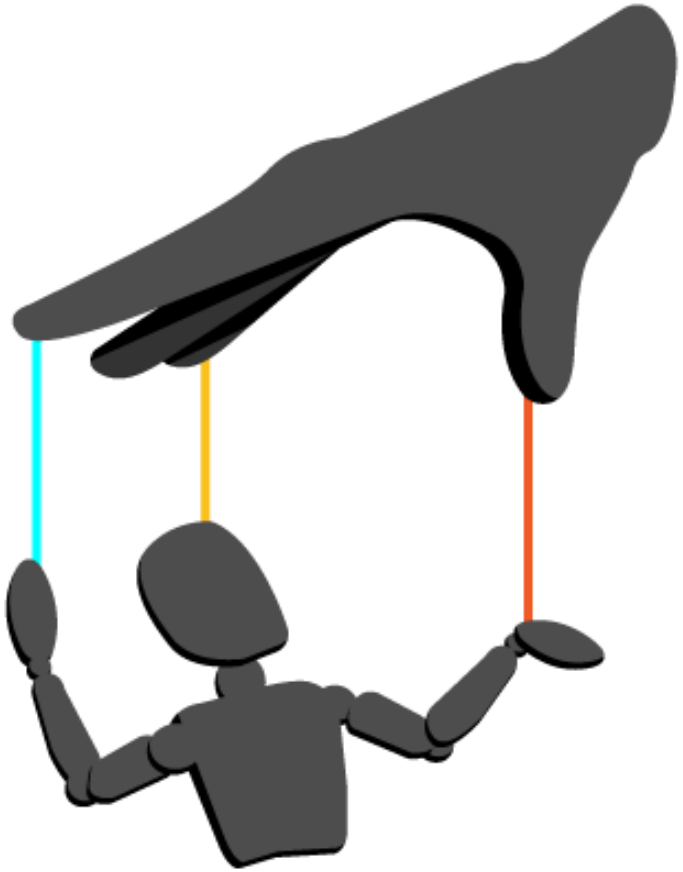
Workshop

Presented by Dr: **Brahim Ferik**

- This workshop covers crucial areas of modern cybersecurity and digital forensics: social engineering email phishing, digital file analysis, and network attacks. Participants will learn how to identify, analyze, and mitigate common threats through practical methods, forensic tools, and investigation strategies, preparing them to handle various security incidents.

- https://shorturl.at/8q8Nk

SOCIAL ENGINEERING



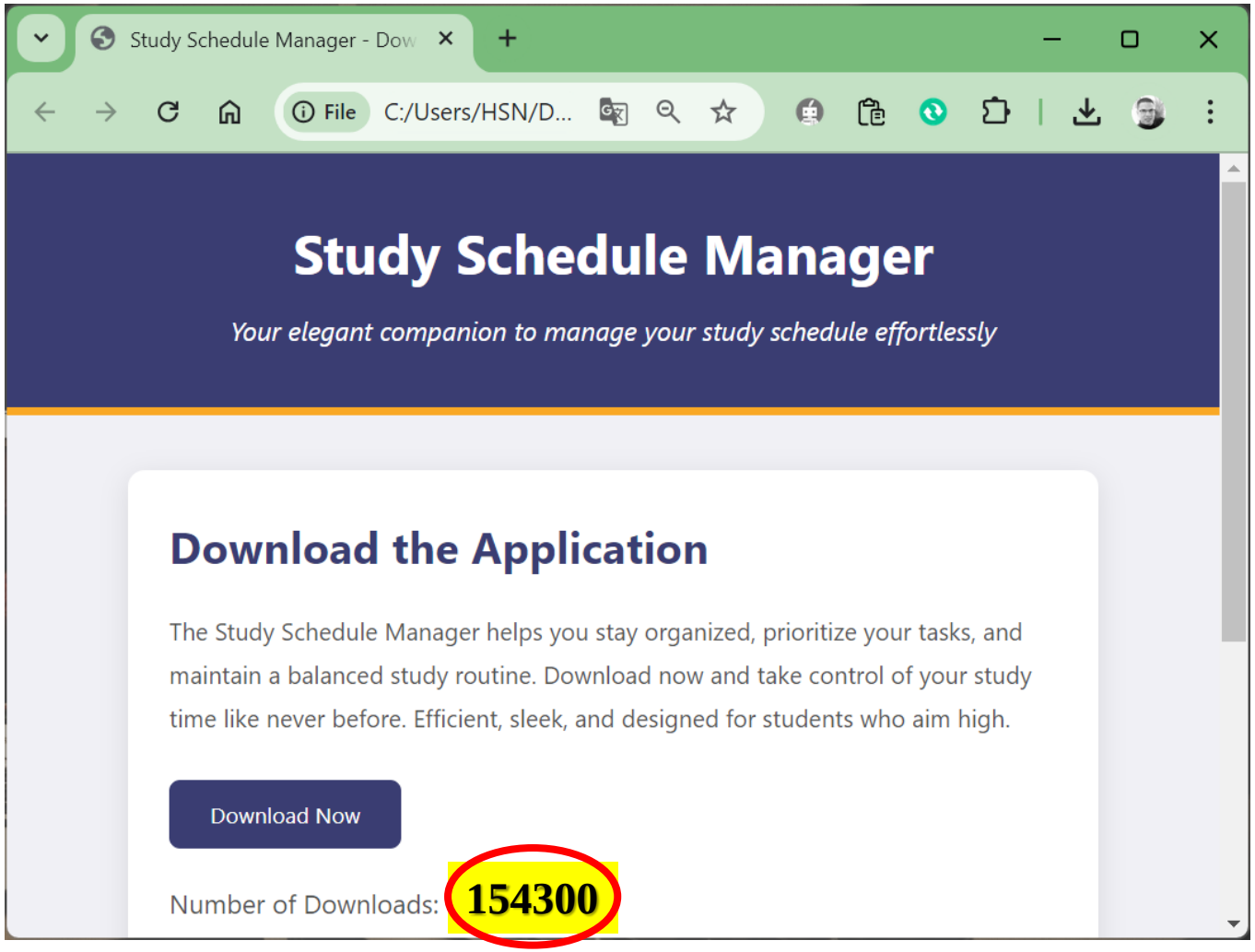
SOCIAL ENGINEERING

- Social engineering is a deceptive tactic exploiting human psychology to gain unauthorized access or information. Unlike technical hacking, it manipulates people through trust, urgency, or emotion. Attackers may impersonate authorities, create false scenarios, or use persuasion to bypass security.

PSYCHOLOGICAL TECHNIQUES

- ❑ **Trust**
- ❑ **Urgency**
- ❑ **Baiting**
- ❑ **Phishing**
- ❑ **Consensus**
- ❑ **Fear**

EXAMPLE OF CONSENSUS

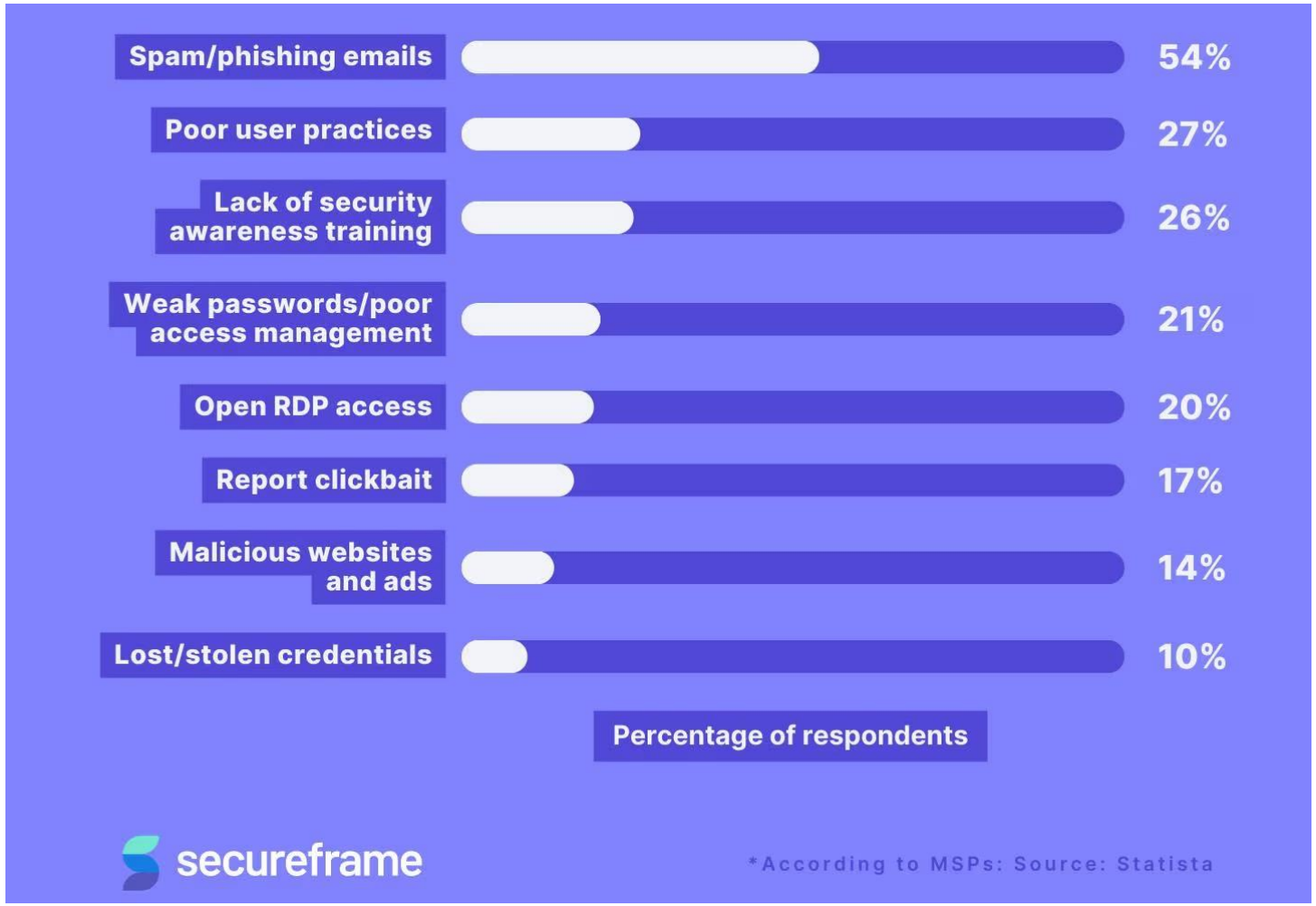


SOCIAL MEIDA CYBER DEFENCE

THE FOUR PHASES OF A SOCIAL ENGINEERING ATTACK

- ❑ **Discovery and investigation**
- ❑ **Deception and hook**
- ❑ **Attack**
- ❑ **Retreat**

PHISHING STATISTICS



PHISHING EMAIL ANALYSIS

SIMPLE EMAIL HEADER

Alice <alice@example.org>

to me

from:	**Alice** <alice@example.org>
to:	Bob <bob@example.com>
date:	Oct 28, 2020, 9:37 AM
subject:	Here we go again
mailed-by:	example.org
signed-by:	example.org
security:	Standard encryption (TLS) Learn more

EMAIL FILE HEADER

Original Message

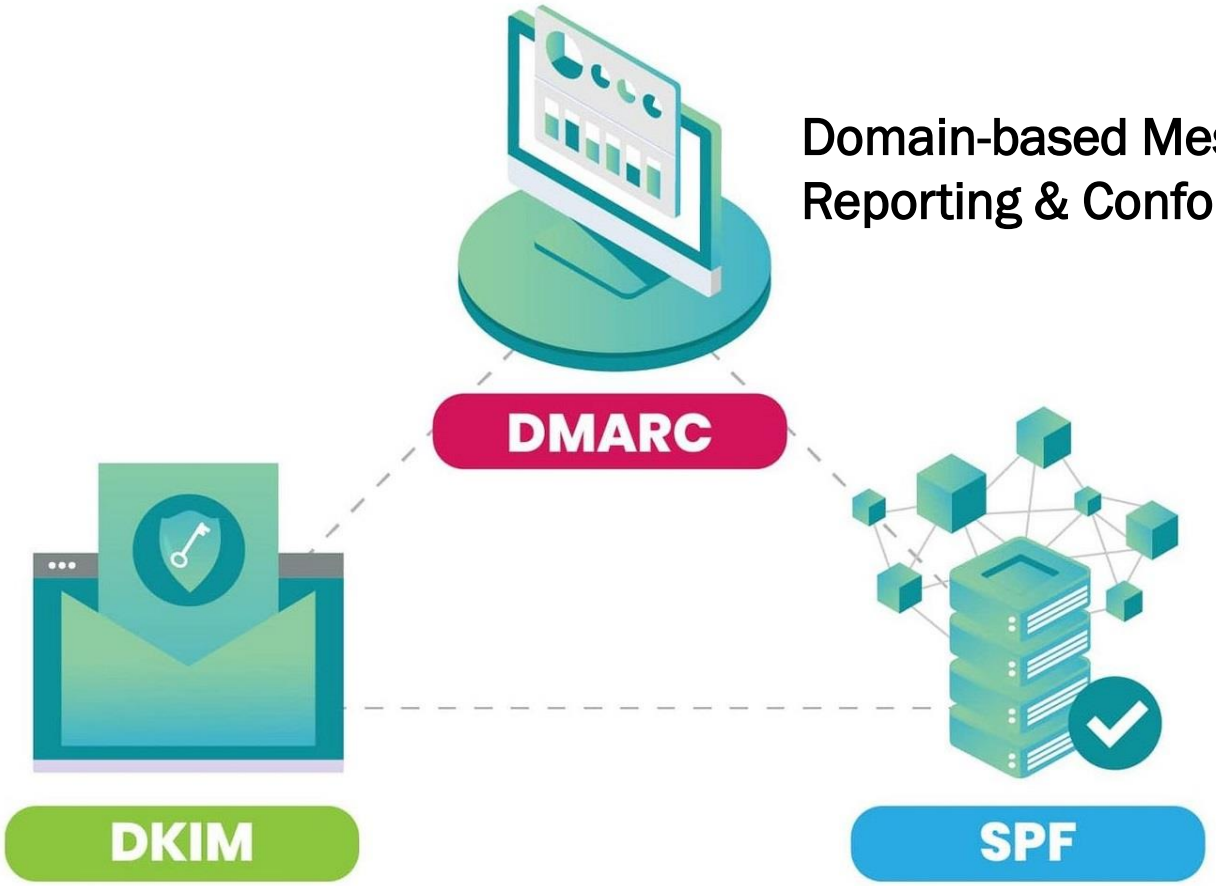
Message ID	<7a159a20-60de-4135-9610-4b42f14b85e0@ind1s01mta1231.xt.local>
Created at:	Thu, Jan 19, 2023 at 10:55 PM (Delivered after 12 seconds)
From:	Slack <no-reply@email.slackhq.com>
To:	bernard@omnisend.com
Subject:	How to start a conversation in Slack
SPF:	PASS with IP 136.147.187.247 Learn more
DKIM:	'PASS' with domain email.slackhq.com Learn more
DMARC:	'PASS' Learn more

Download Original

Copy to clipboard

SOCIAL MEIDA CYBER DEFENCE

EMAIL AUTHENTICATION METHODS



Domain-based Message Authentication, Reporting & Conformance

DomainKeys Identified Mail

Sender Policy Framework

TOOLS FOR EMAIL HEADER ANALYSIS

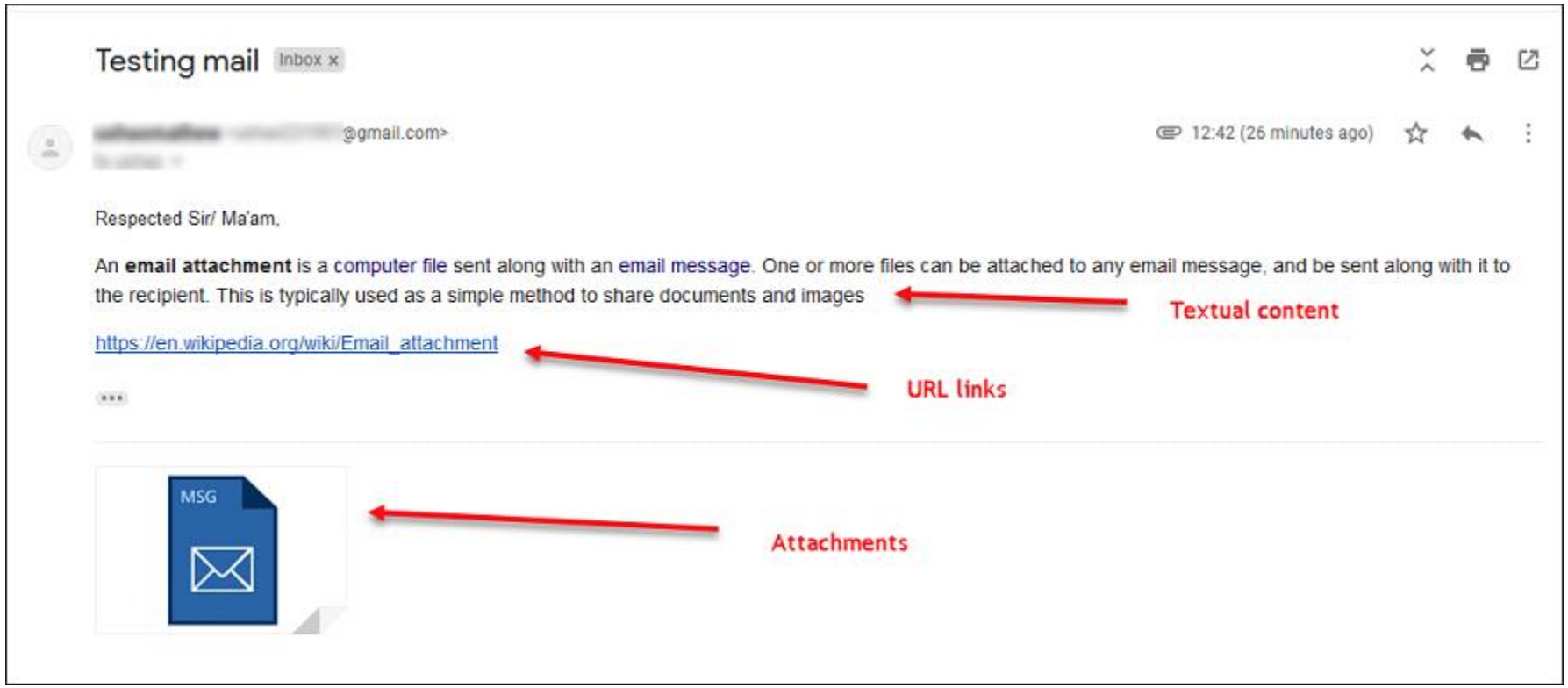
VIRUSTOTAL

MX TOOLBOX®

DMARCLY

SOCIAL MEIDA CYBER DEFENCE

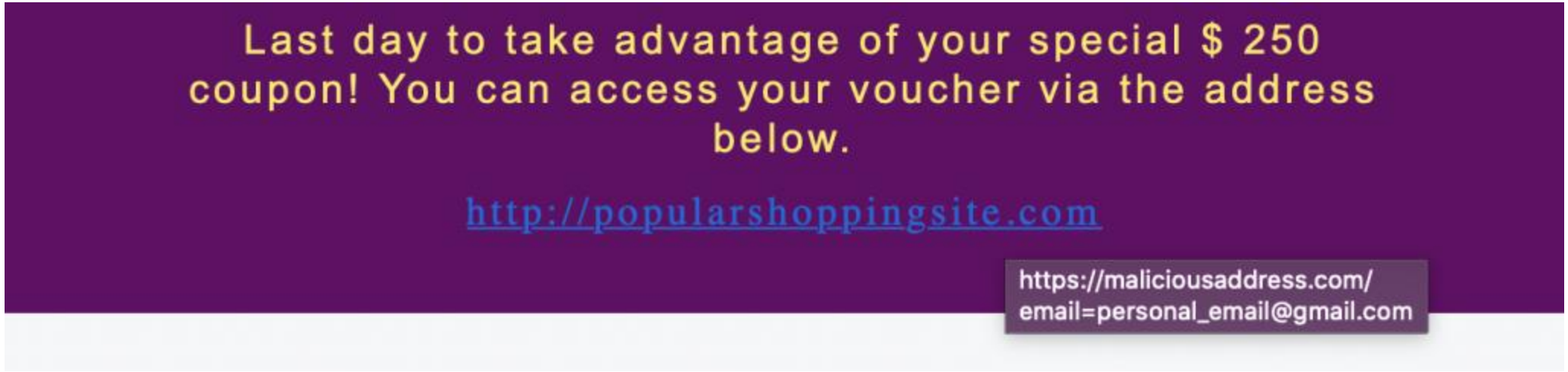
EMAIL CONTENT ANALYSIS



BASIC STRUCTURE OF EMAIL FILE

- **Content-Type** is **application/pdf**.
- **Content-Disposition** specifies it's an **attachment.**
- **Content-Transfer-Encoding** tells us it's **base64 encoded.**

HTML EMAILS SUPPORT



READING URLS TO AVOID PHISHING SCAMS

Incorrectly spelled domain names:

- ❑ google.com
- ❑ facebo0k.com
- ❑ amzon.com
- ❑ appel.com
- ❑ micorsoft.com

Domain Jumble:

No Single
Forward-Slash

https://www.facebook.com

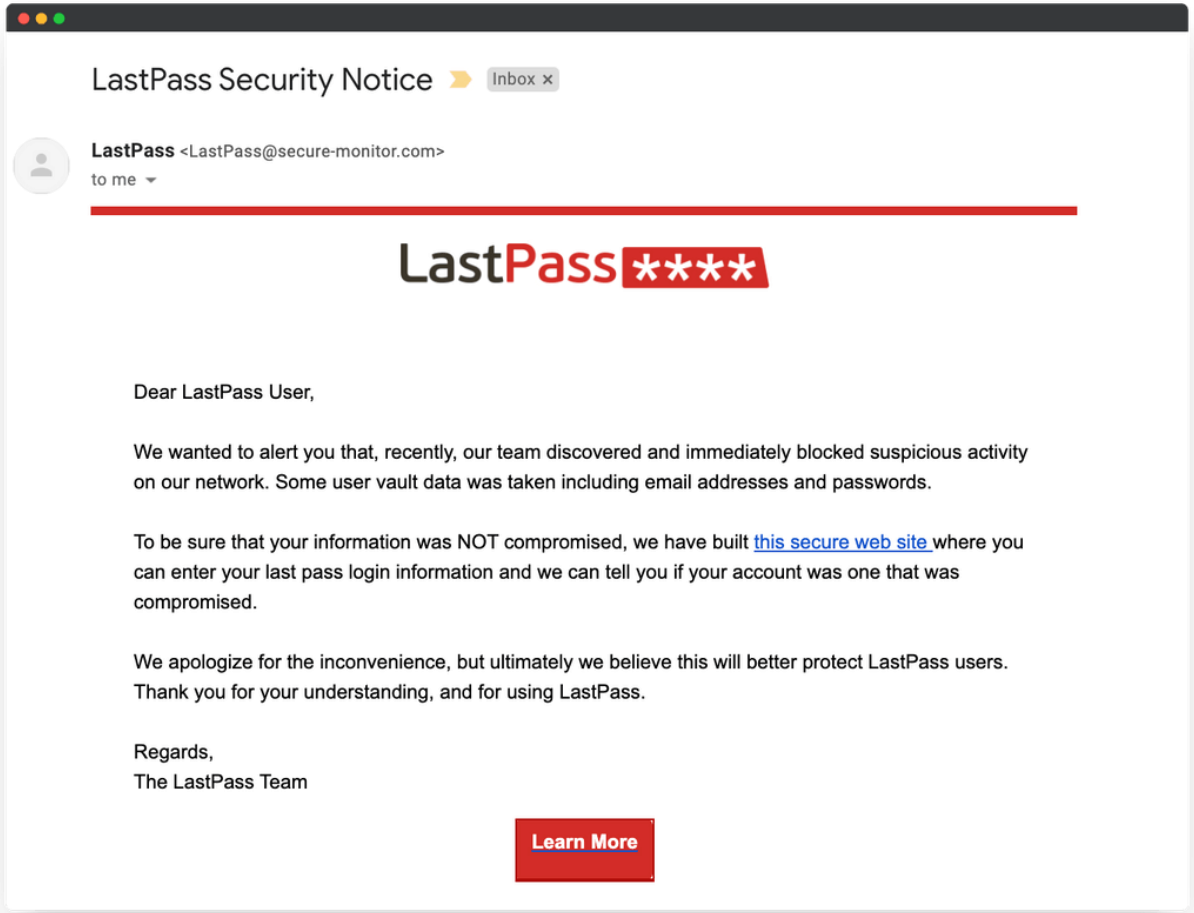
Top-Level Domain

First Single
Forward-Slash

http://activate.facebook.fblogins.net/8675309/activate.php

Top-Level Domain

PHISHING EMAIL EXAMPLE



LastPass Security Notice Inbox ×

LastPass <LastPass@secure-monitor.com>
to me

LastPass ****

Dear LastPass User,

We wanted to alert you that, recently, our team discovered and immediately blocked suspicious activity on our network. Some user vault data was taken including email addresses and passwords.

To be sure that your information was NOT compromised, we have built this secure web site where you can enter your last pass login information and we can tell you if your account was one that was compromised.

We apologize for the inconvenience, but ultimately we believe this will better protect LastPass users. Thank you for your understanding, and for using LastPass.

Regards,
The LastPass Team

Learn More

SOCIAL MEIDA CYBER DEFENCE

PHISHING EMAIL EXAMPLE

LinkedIn Alert: Account Flagged Inbox ×

LinkedIn Sales Navigator <noreply@account-services-linkedin.com>
to me

LinkedIn
Sales Navigator

Dear Member,

This is an important message. Your membership on LinkedIn has been flagged for too reasons, the use of a different IP address and a login on a new device.

Our system indicates your account signed-on from a different IP address recently. We advise you to kindly follow up by updating the system to enable "auto unflag" and your account access will be recognized again. Verifying your LinkedIn access with the email address provided will help to avoid future difficulties with LinkedIn services.

Continue to review the activity by following the secure link below:

LinkedIn Security Center

Thank you for using LinkedIn.

The LinkedIn Team

This message is an important message from LinkedIn and if not attended to, may lead to account suspension or closure!

SOCIAL MEIDA CYBER DEFENCE

PHISHING EMAIL EXAMPLE

LinkedIn Alert: Account Flagged Inbox ×

LinkedIn Sales Navigator <noreply@account-services-linkedin.com>
to me

LinkedIn Sales Navigator

Dear Member,

This is an important message. Your membership on LinkedIn has been flagged for too reasons, the use of a different IP address and a login on a new device.

Our system indicates your account signed-on from a different IP address recently. We advise you to kindly follow up by updating the system to enable "auto unflag" and your account access will be recognized again. Verifying your LinkedIn access with the email address provided will help to avoid future difficulties with LinkedIn services.

Continue to review the activity by following the secure link below:

LinkedIn Security Center

Thank you for using LinkedIn.

The LinkedIn Team

This message is an important message from LinkedIn and if not attended to, may lead to account suspension or closure!

SOCIAL MEIDA CYBER DEFENCE

PHISHING INDICATORS

- The sender's email address is not associated with the company.
- The email uses a fake company logo.
- does not mention any specific details.
- The email contains grammatical errors.

PHISHING EMAIL EXAMPLE

This is one example of an improved phishing email.
There are many different ways you could have done this.

Spelling of Mastercard fixed and email comes from a relatable address

From: Mastercard Staff Rewards
To: employee@email.com
Subject: Your Black Friday Employee reward card
—

Email is personalized and poor grammar is fixed

Body:
Hello <name>,

Contextualize to upcoming Black Friday event

In recognition of your hard work throughout the year, we wish to reward you with a gift card to spend in the upcoming Black Friday sales as a small token of our appreciation. Please find attached your Employee reward card.

Link is masked in plaintext to hide phishing link

The balance of your card will be determined based on your role. To view the balance and activate your employee reward card, visit here.

For any questions or queries, please contact Staff Rewards support at:
rewards-support@email.com

To increase legitimacy, buffer text is added

From,
Staff Reward Services

CONFIDENTIAL: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

Simple confidentiality disclaimer to add legitimacy to email.
This was taken from an article on Exclaimer.com

SOCIAL MEIDA CYBER DEFENCE

REAL-LIFE SCENARIO

- emkei.cz

- temp-mail.org

Fake email generator

- https://shorturl.at/kXTV8

PHISHING EMAIL ANALYSIS

PHISHING EMAIL INVESTIGATION:

A PRACTICAL EXERCISE

PHISHING EMAIL ANALYSIS

PHISHTOOL

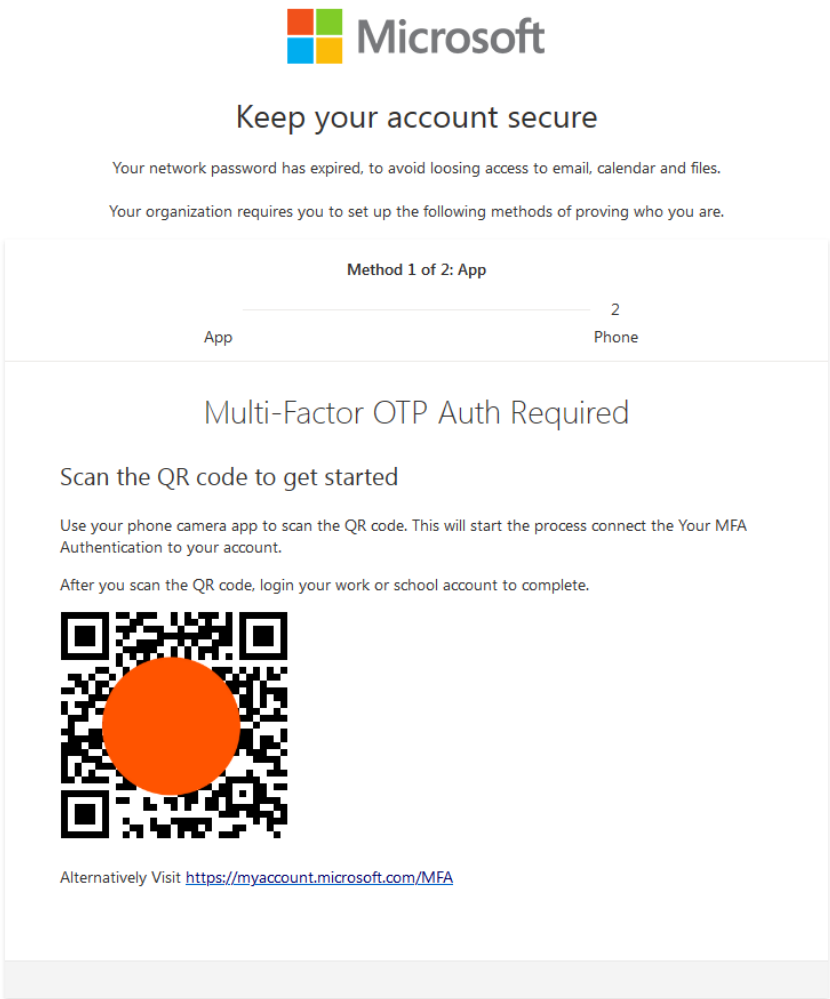
The power to reverse engineer phishing emails

QUISHING

SCAN ME

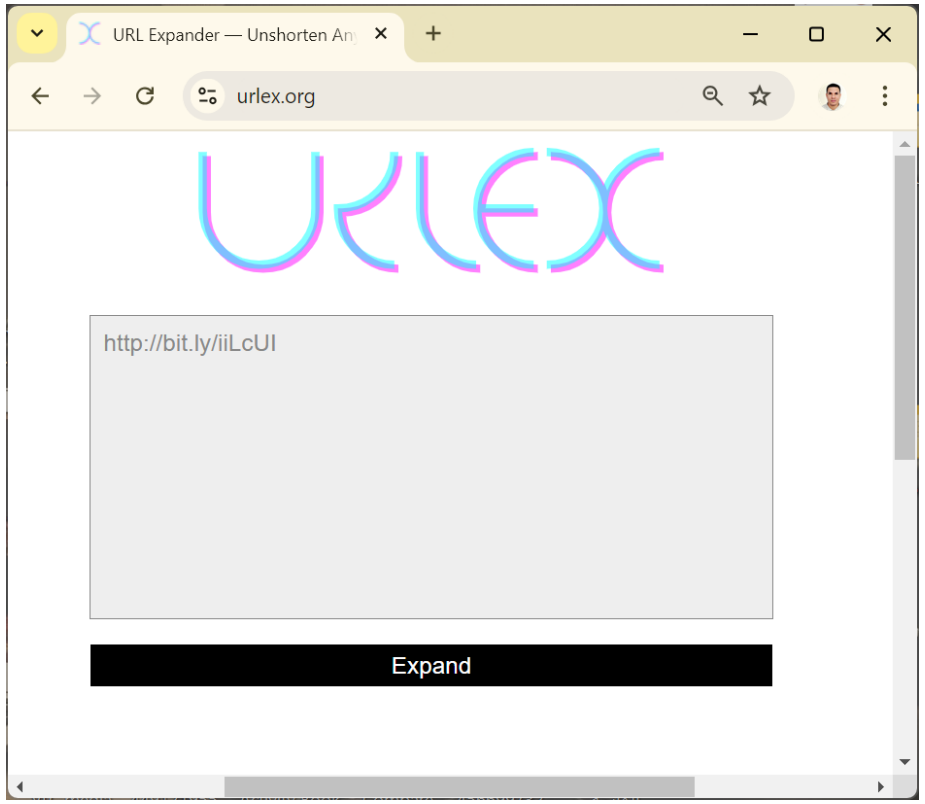
QUISHING


https://crello.com/user/projects/5ce172b06511c5002b4da
Shorten URL and Copy to Clipboard
https://is.gd/mRmYvq
Rate Us
Generate QR Code
History


Microsoft
Keep your account secure
Your network password has expired, to avoid loosing access to email, calendar and files.
Your organization requires you to set up the following methods of proving who you are.
Method 1 of 2: App
App
2
Phone
Multi-Factor OTP Auth Required
Scan the QR code to get started
Use your phone camera app to scan the QR code. This will start the process connect the Your MFA Authentication to your account.
After you scan the QR code, login your work or school account to complete.
Alternatively Visit https://myaccount.microsoft.com/MFA

QUISHING SIMULATION PROCESS

Short URL



PROTECTIVE MEASURES

- ❑ **Verify the Source of a QR Code**
- ❑ **Preview the Destination URL**
- ❑ **Update your device's security and overall defense system**

THE TOP SOCIAL ENGINEERING TOOLS

- ❑ SET (Social-Engineer Toolkit)
- ❑ GoPhish
- ❑ HiddenEye
- ❑ BeEF (Browser Exploitation Framework)
- ❑ Beelogger
- ❑ Evilginx

REFERENCES

- https://mailtrap.io/blog/email-headers/
- https://app.letsdefend.io/training/lesson_detail/email-header-analysis
- https://medium.com/@DaoudaD/basic-analysis-of-a-phishing-email-fbe2276a7d67

COMMON VULNERABILITIES AND EXPOSURES (CVE)

Common Vulnerabilities and Exposures

COMMON VULNERABILITIES AND EXPOSURES (CVE)

- ❑ **Standardization**
- ❑ **Ease of Management**

WHERE TO FIND CVE LISTINGS

- ❑ **MITRE CVE Database**
- ❑ **National Vulnerability Database (NVD)**
- ❑ **Security advisories from software vendors**

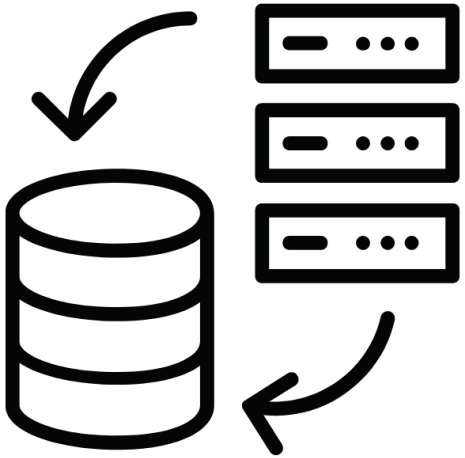
HOW TO EXPLOIT A CVE

- ❑ **Research**
- ❑ **Environment Setup**
- ❑ **Tools**
- ❑ **Execution**
- ❑ **Analysis**

UPDATE SOFTWARE

DATA BACKUP STRATEGIES

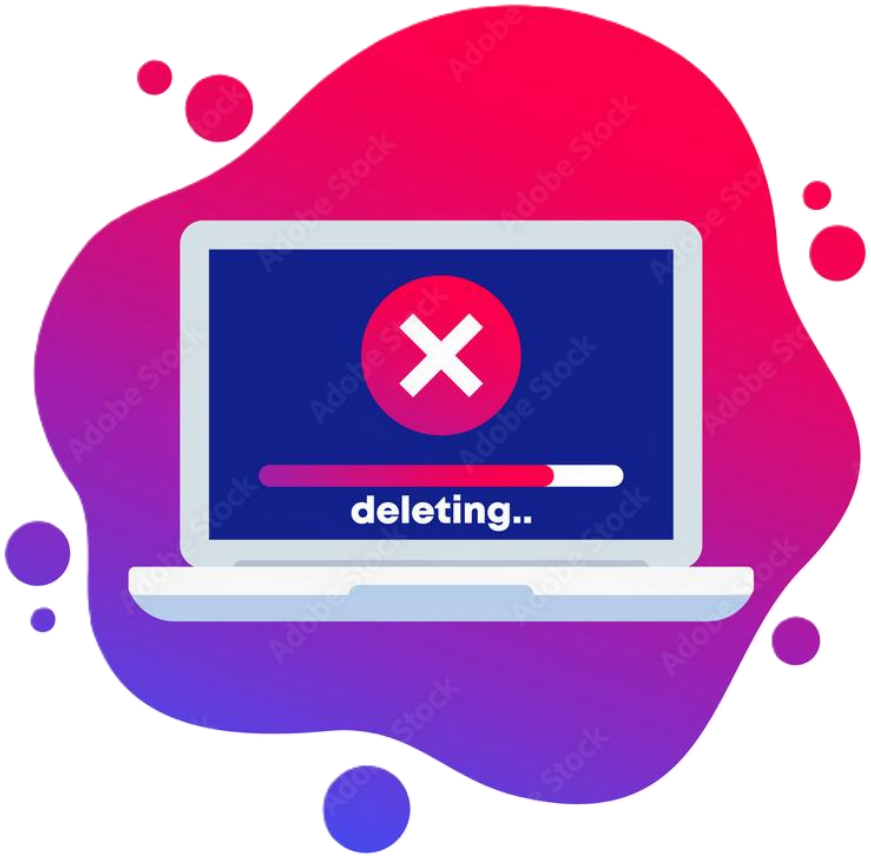
www.duplicati.com



DELETE DATA PERMANENTLY

eraser.heidi.ie

www.fileshredder.org



BEST PRACTICES FOR MALWARE SCANNING

SOCIAL MEIDA CYBER DEFENCE

BEST PRACTICES FOR MALWARE SCANNING

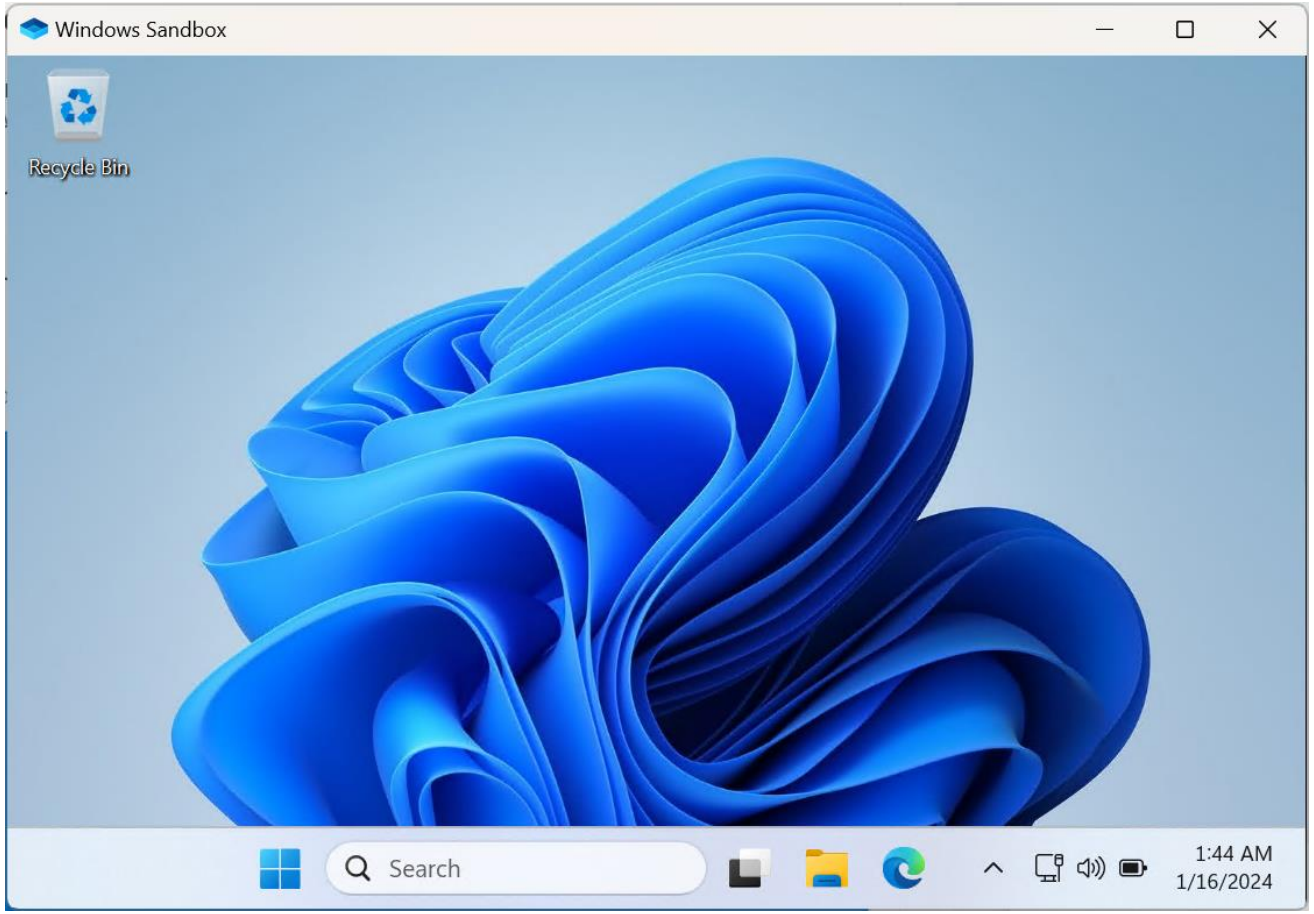
virustotal.com

any.run

www.hybrid-analysis.com

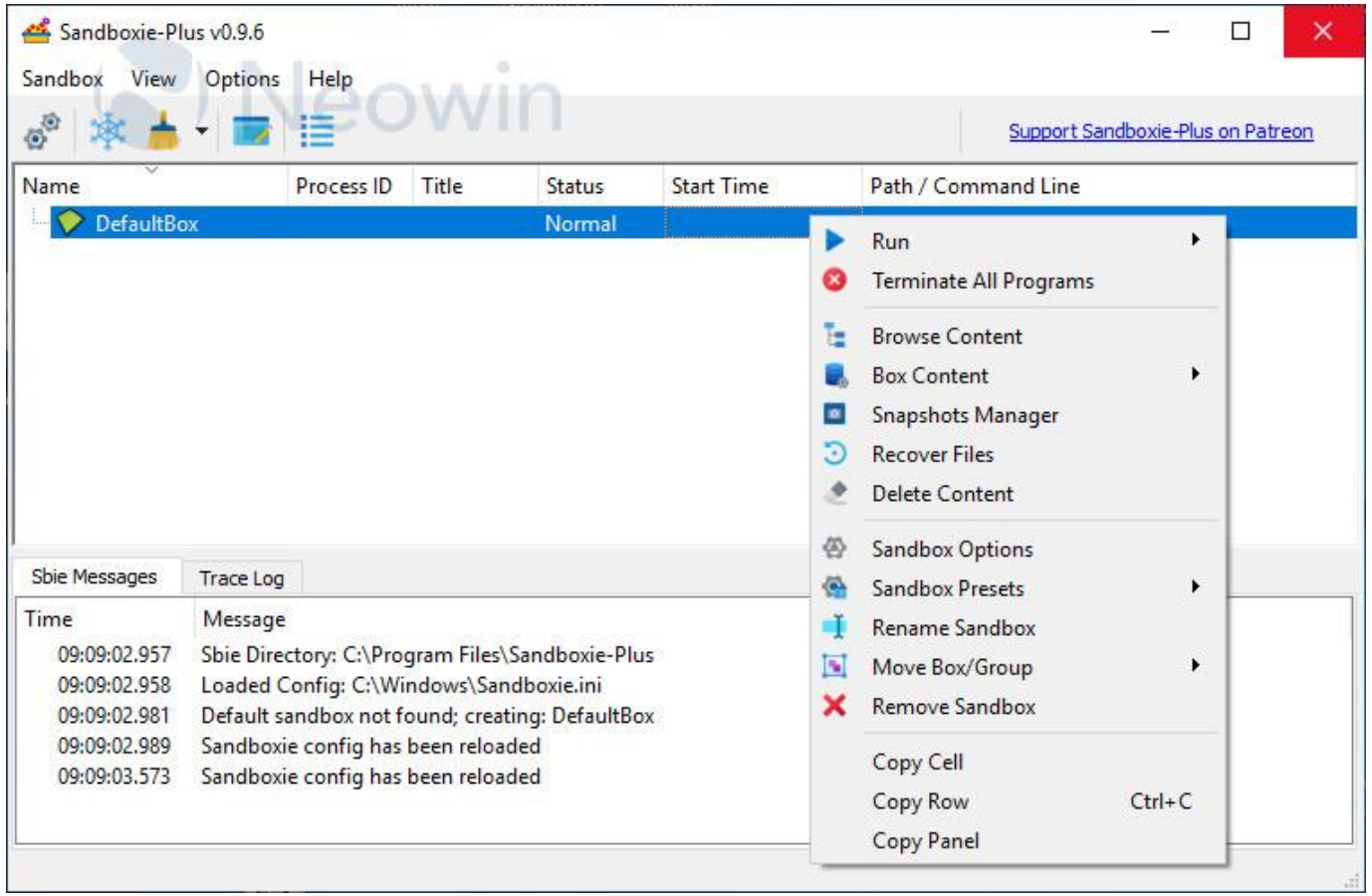
virusscan.jotti.org

BEST PRACTICES FOR MALWARE SCANNING



SOCIAL MEIDA CYBER DEFENCE

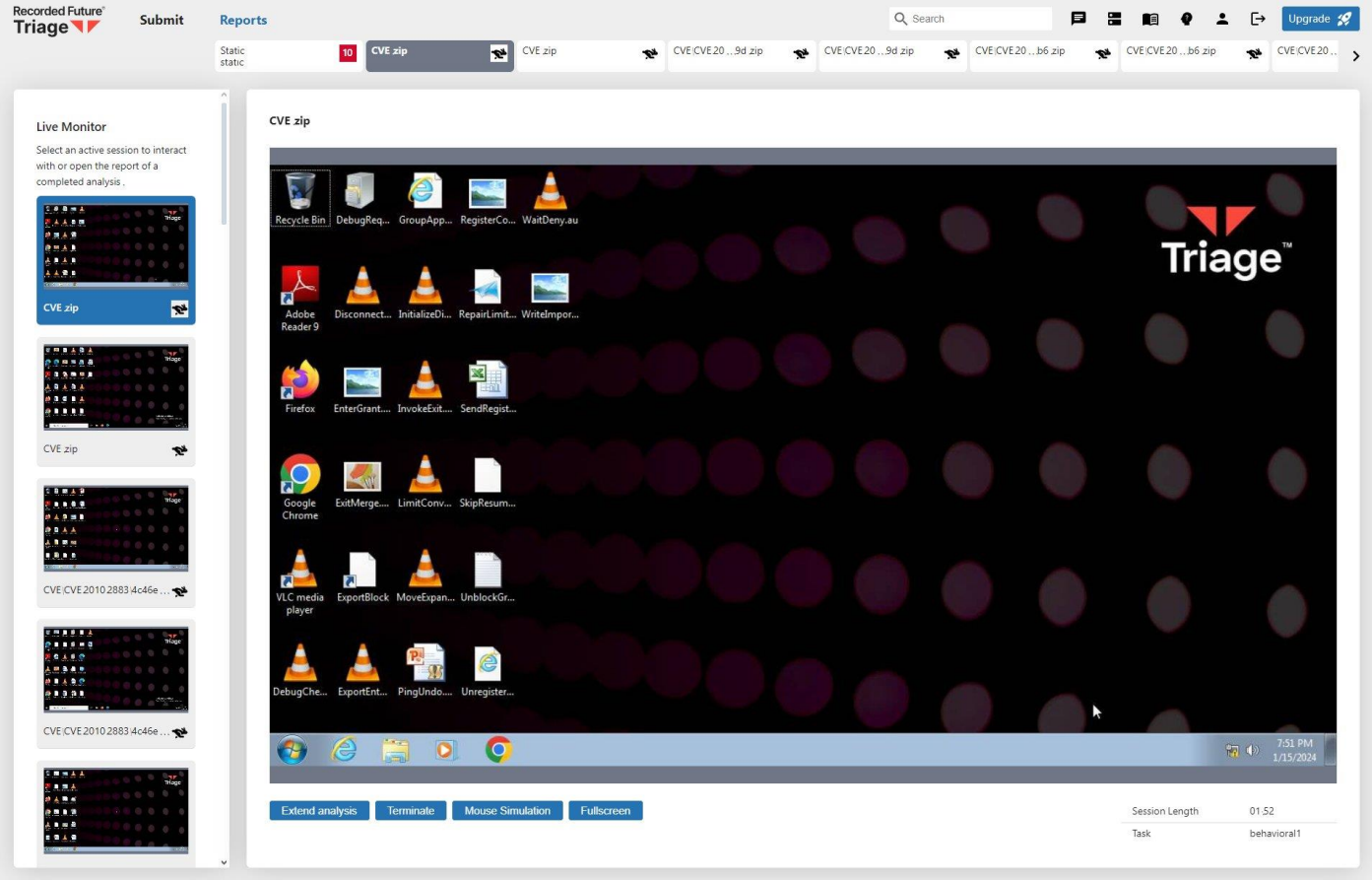
BEST PRACTICES FOR MALWARE SCANNING



BEST PRACTICES FOR MALWARE SCANNING

Recorded Future Triage

Tria.ge



BEST PRACTICES FOR MALWARE SCANNING

https://shorturl.at/Y3zrL

BEST PRACTICES FOR MALWARE SCANNING

https://shorturl.at/kD6RY

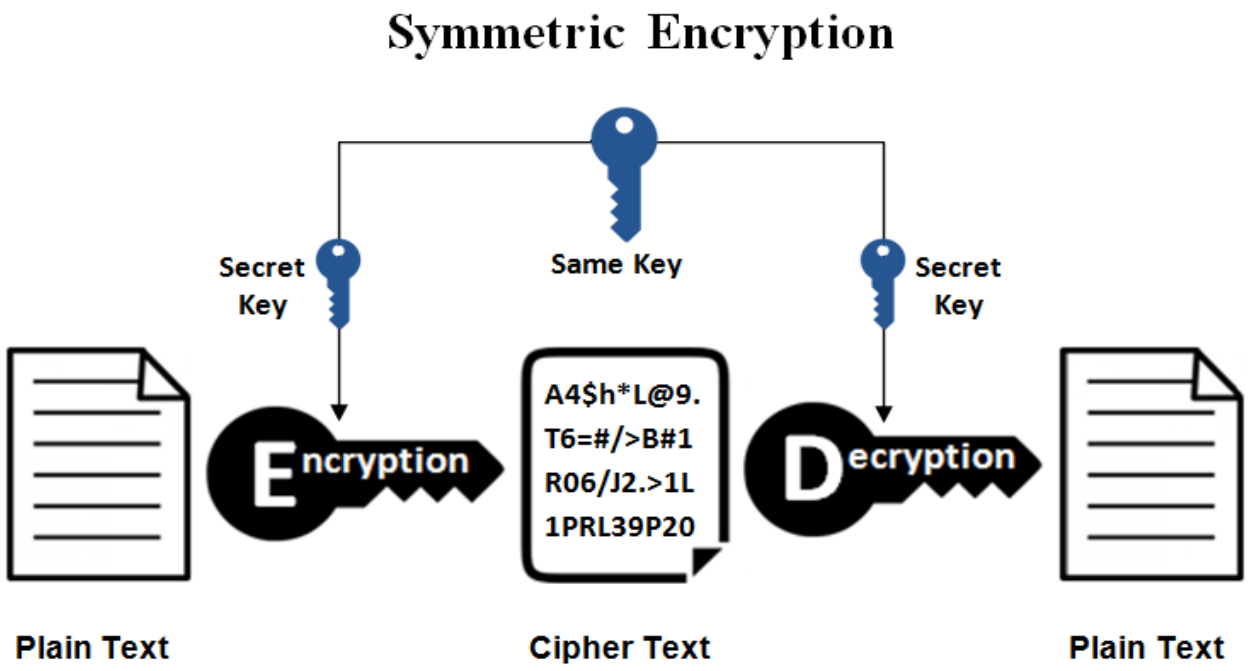
BEST PRACTICES FOR MALWARE SCANNING

- bazaar.abuse.ch
- github.com/ytisf/theZoo
- github.com/jstrosch/malware-samples

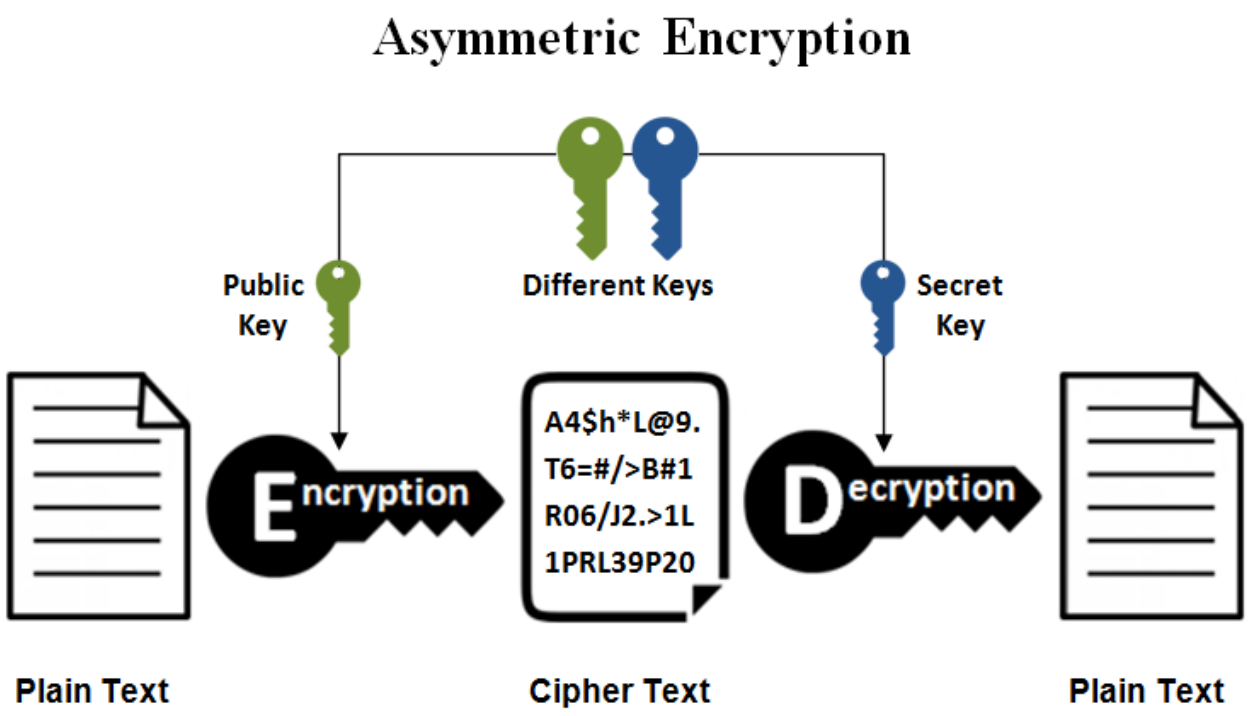
DIGITAL FILE ANALYSIS AND INFORMATION EXTRACTION

- **Digital File Analysis and Information Extraction are critical in modern investigations, enabling professionals to uncover hidden or protected data within suspicious files. In this workshop, participants learn essential techniques, from recognizing file signatures to extracting metadata and recovering passwords from encrypted archives, ensuring forensic outcomes.**

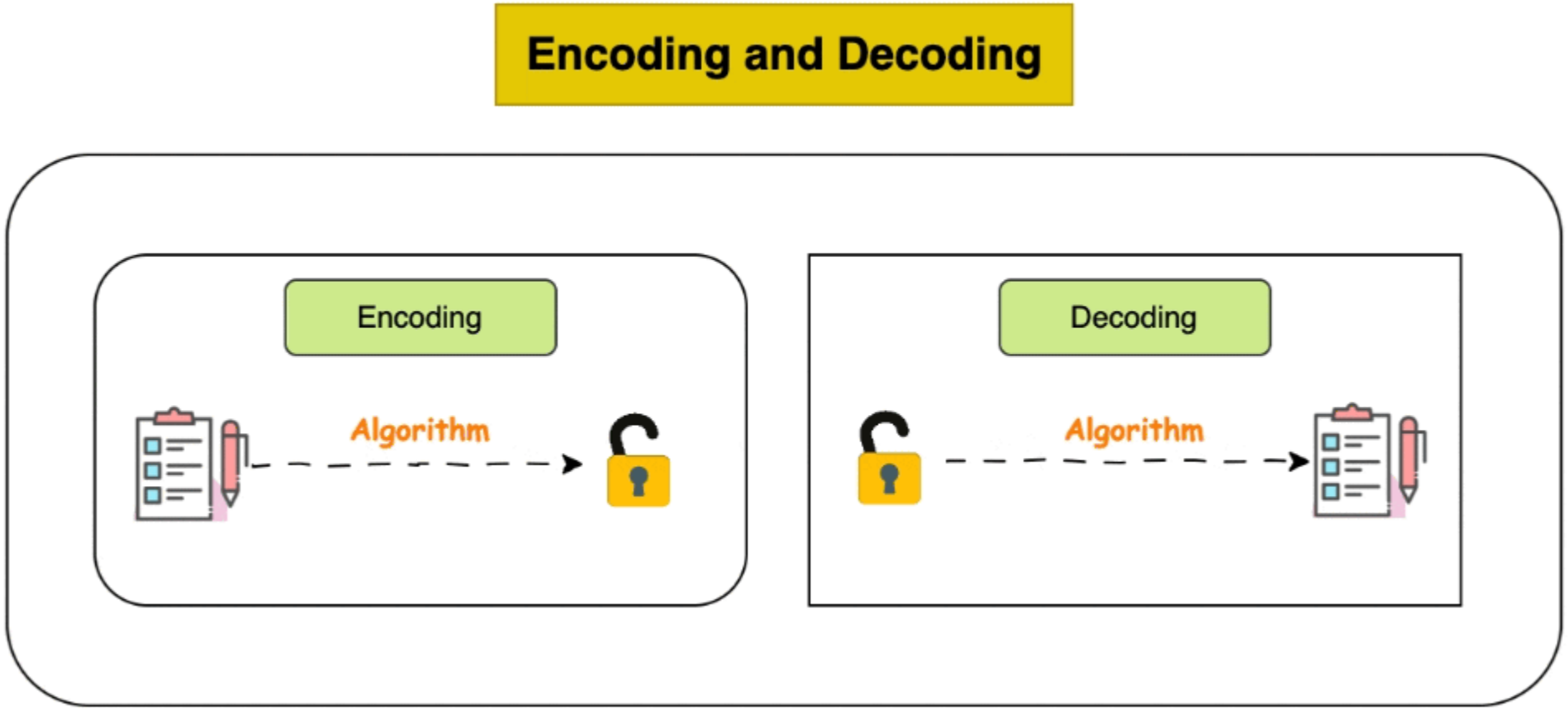
ENCRYPTION, ENCODING AND HASHING



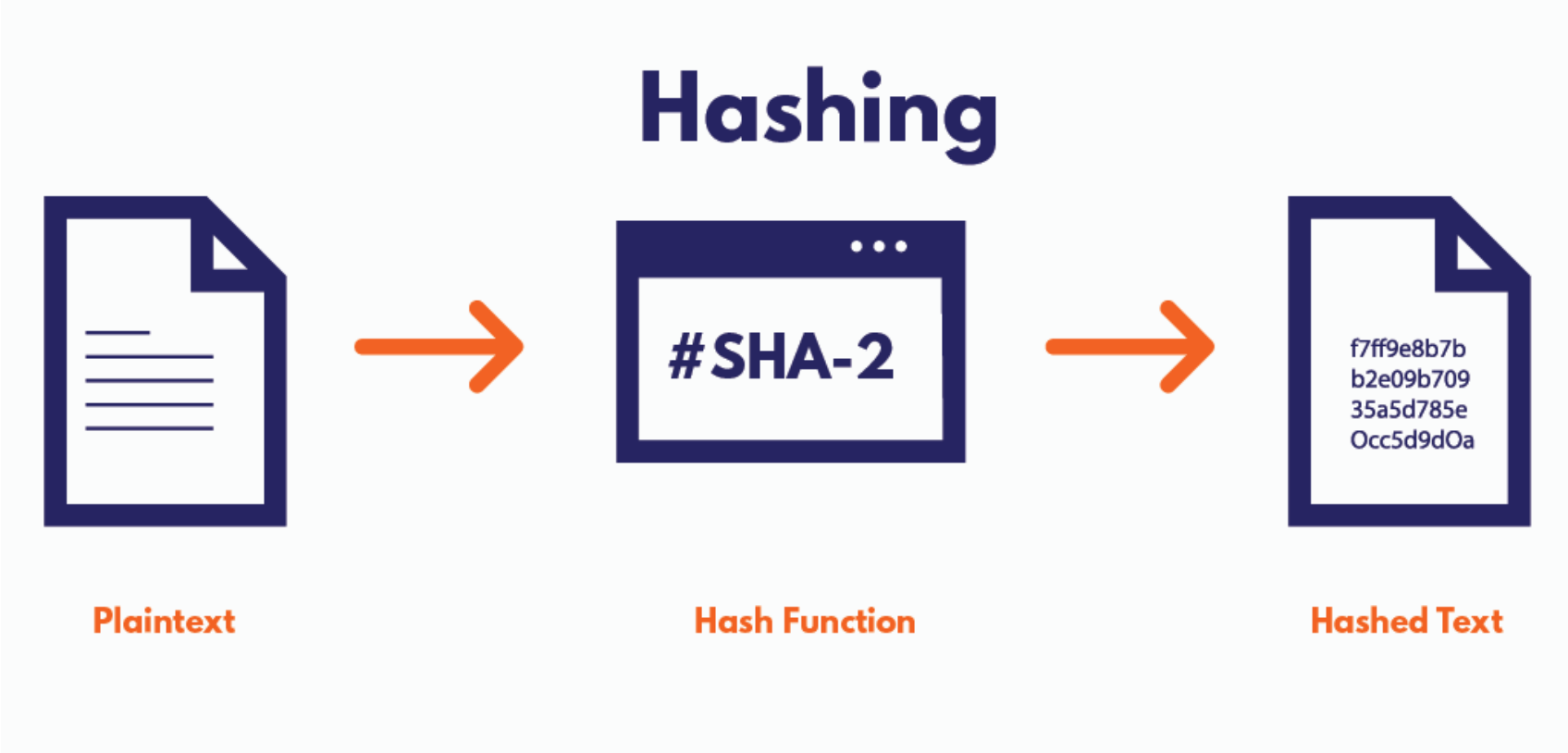
ENCRYPTION, ENCODING AND HASHING



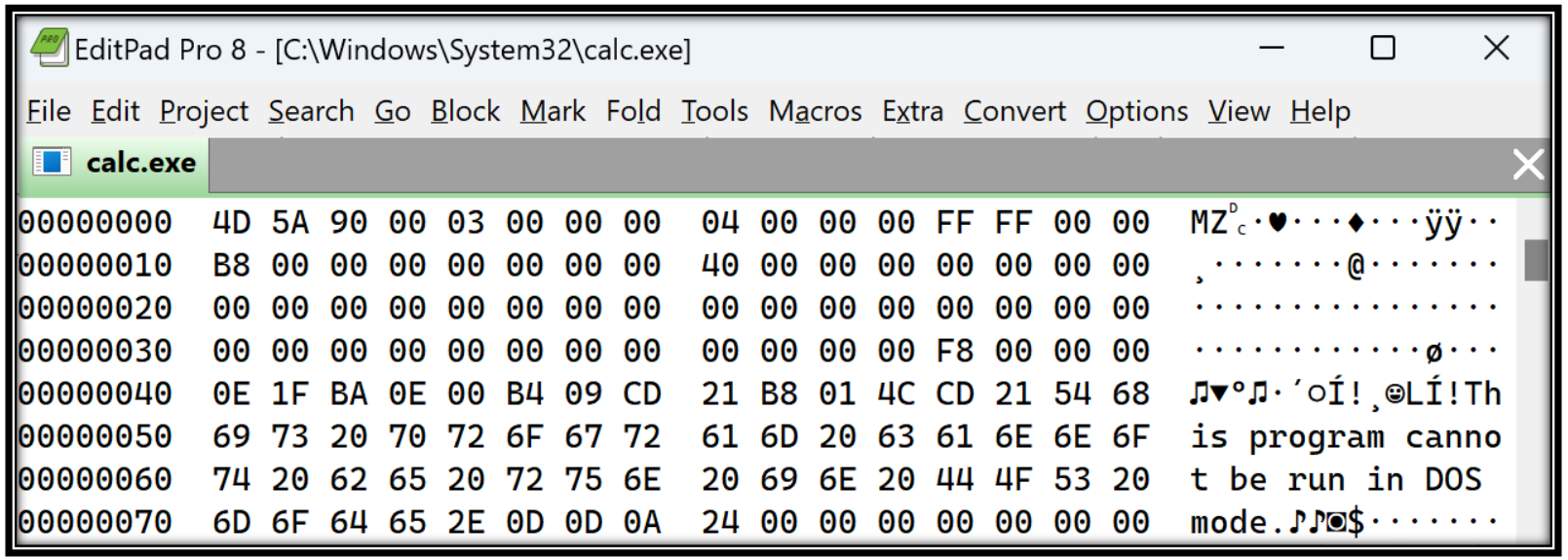
ENCRYPTION, ENCODING AND HASHING



ENCRYPTION, ENCODING AND HASHING



UNDERSTANDING FILE TYPES AND MAGIC NUMBERS



EXTRACTING METADATA FROM IMAGES

TYPES OF FILE PROTECTION AND ENCRYPTION METHODS

- **Key Techniques**

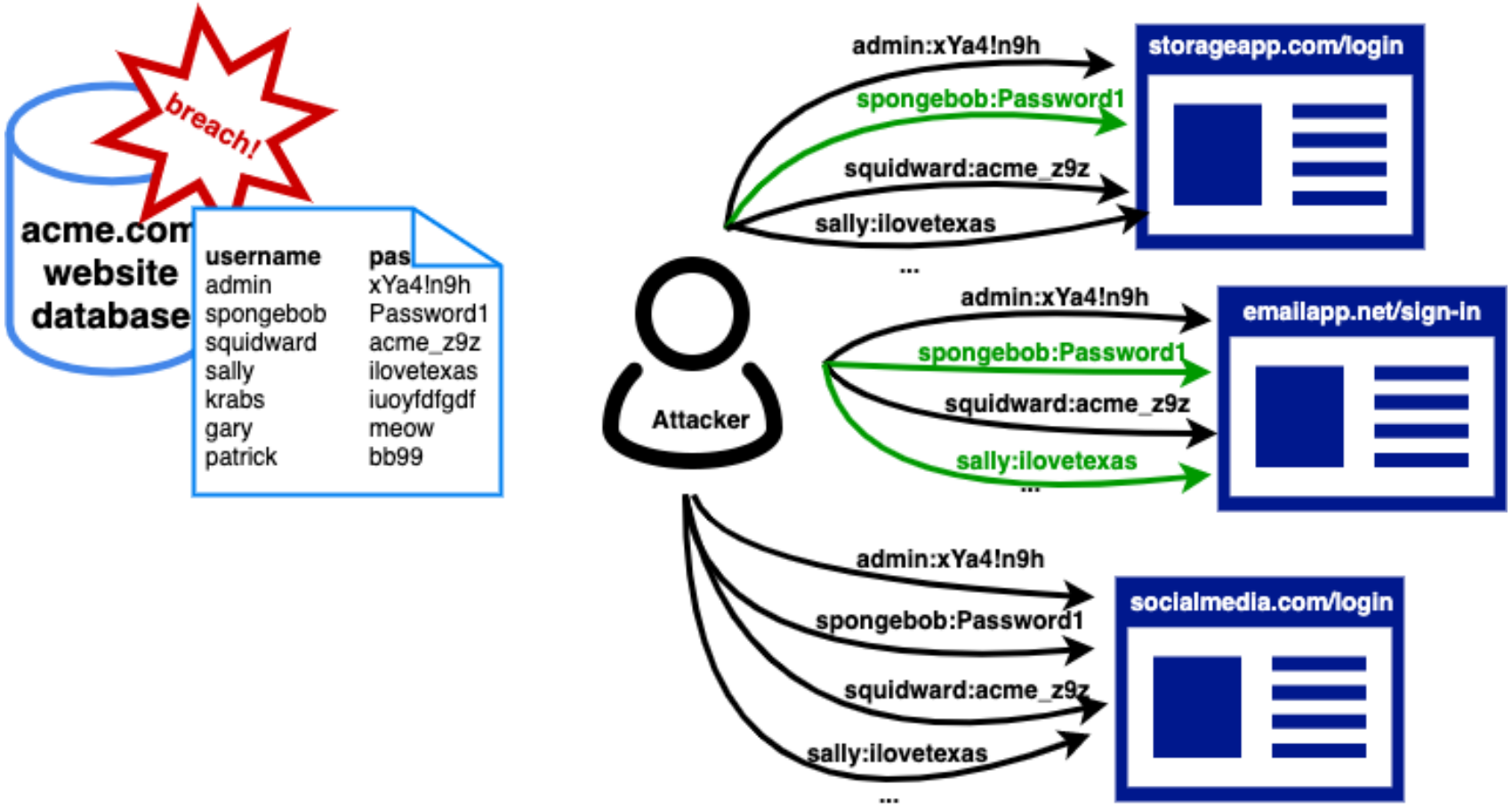
- ❑ **Password Protection.**
- ❑ **Hash-based Verification.**
- ❑ **Full Encryption.**

PASSWORD CRACKING TECHNIQUES FOR PROTECTED FILES

- **Key Techniques**

- ❑ **Dictionary Attacks.**
- ❑ **Combinator Attacks.**
- ❑ **Brute-force Attacks.**
- ❑ **Phishing/Social Engineering.**
- ❑ **Credential Stuffing.**

PASSWORD CRACKING METHODS



PASSWORD CRACKING METHODS

PASSWORD CRACKING METHODS

- **Applied Work (Zip file)**

- ❑ **john.exe –list=formats**
- ❑ **zip2john.exe protected.zip>zip.hash**
- ❑ **john.exe zip.hash**

PASSWORD CRACKING METHODS

- **Applied Work (rar file)**

- rar2john.exe protected.rar
- hashcat.exe -m 13000 -a3 value_hash ?d?d?d?d
- hashcat.exe –show -m 13000 value_hash
- https://shorturl.at/icb1C

PASSWORD CRACKING METHODS

- **Applied Work (PDF, DOCX, XLSX, ...)**
- ❑ **Practical Exercises.**
- ❑ **Prepare a wordlist containing common passwords.**

DIGITAL WATERMARKING AS A MEANS OF FILE PROTECTION

- ❑ **Embedded digital information within an image or file**
- ❑ **Does not degrade quality or alter usability**
- ❑ **Used for documentation, tracking, and tamper detection**

IMPORTANCE OF WATERMARKING IN MEDICAL IMAGES

An Efficient Semi-blind Watermarking Technique Based on ACM and DWT for Mitigating Integrity Attacks

Research Article-Computer Engineering and Computer Science | Published: 05 February 2025 (2025) Cite this article

Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia, Abdelkader Laouid, Muath AlShaikh, Khaled Chait & Mohammad Hammoudeh

ELSEVIER

Expert Systems with Applications

Volume 275, 25 May 2025, 126954

An adaptive ACM watermarking technique based on combined feature extraction and non-linear equation

Ahcene Bounceur [a 1], Mostefa Kara [b 1], Brahim Ferik [c 1], Abdelkader Laouid [d 1]

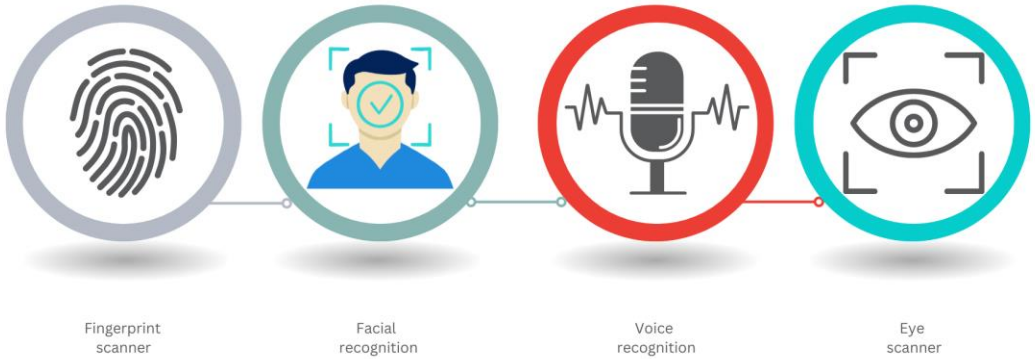
A Multi-Layered Security Framework for Medical Imaging: Integrating Compressed Digital Watermarking and Blockchain

Publisher: IEEE

Cite This PDF

Brahim Ferik ; Lakhdar Laimeche ; Abdallah Meraoumia ; Omar Aldabbas ; Muath AlShaikh ; Abdelkader Laouid

INTEGRATING BIOMETRIC DATA AS A WATERMARK



AI IN WATERMARKING AND VERIFICATION

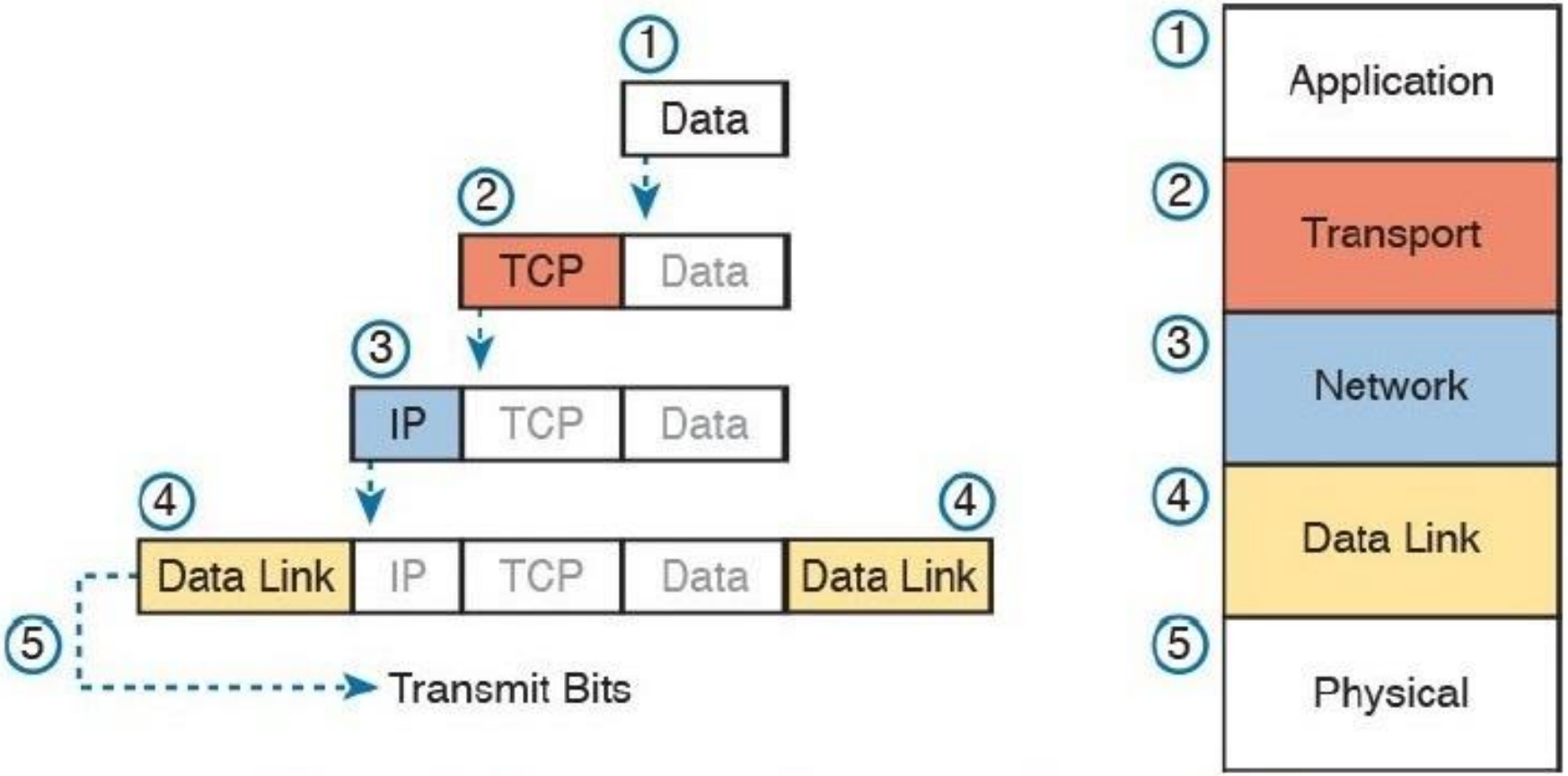
- ❑ **Automated classification of tampered medical images**
- ❑ **Automatic watermark detection**
- ❑ **Quality assessment by comparing original vs. modified images**

WATERMARKING IN CYBERSECURITY AND CRIMINAL JUSTICE

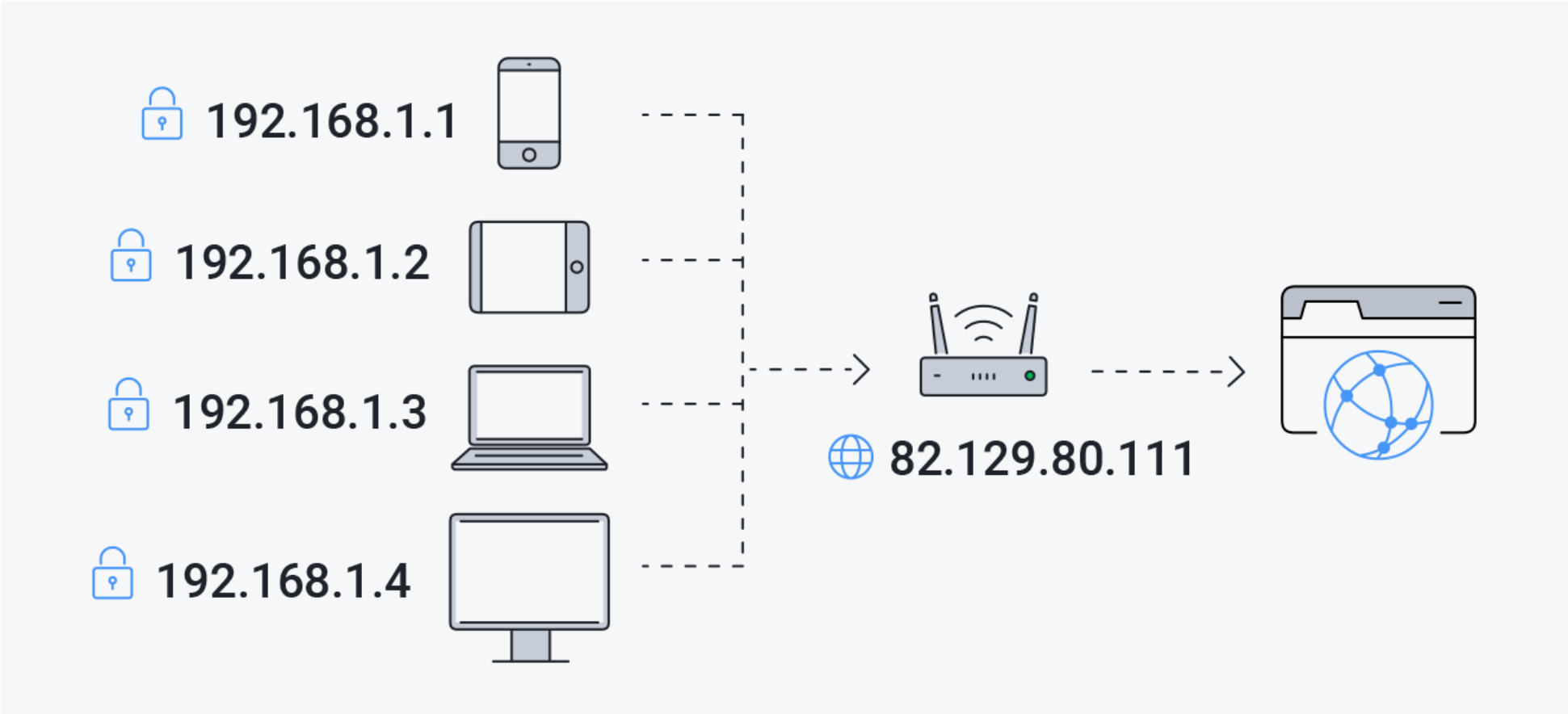
- Digital Evidence Ownership.
- Document Leakage Tracking & Authenticity Verification.
- Medical/Forensic Imaging & Surveillance Videos.
- Anti-forgery & AI-based watermark Detection.

NETWORK ATTACKS ANALYSIS AND INVESTIGATION

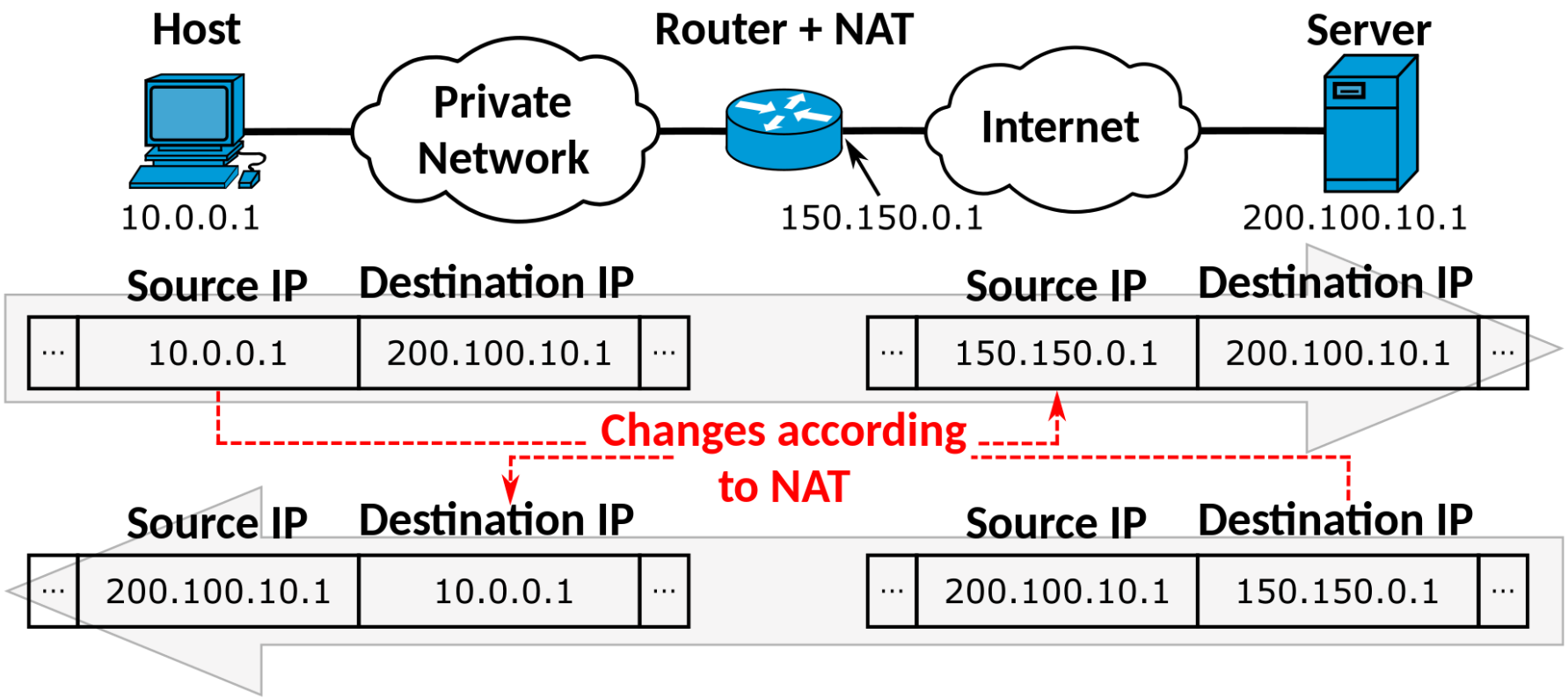
TCP/IP (TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL)



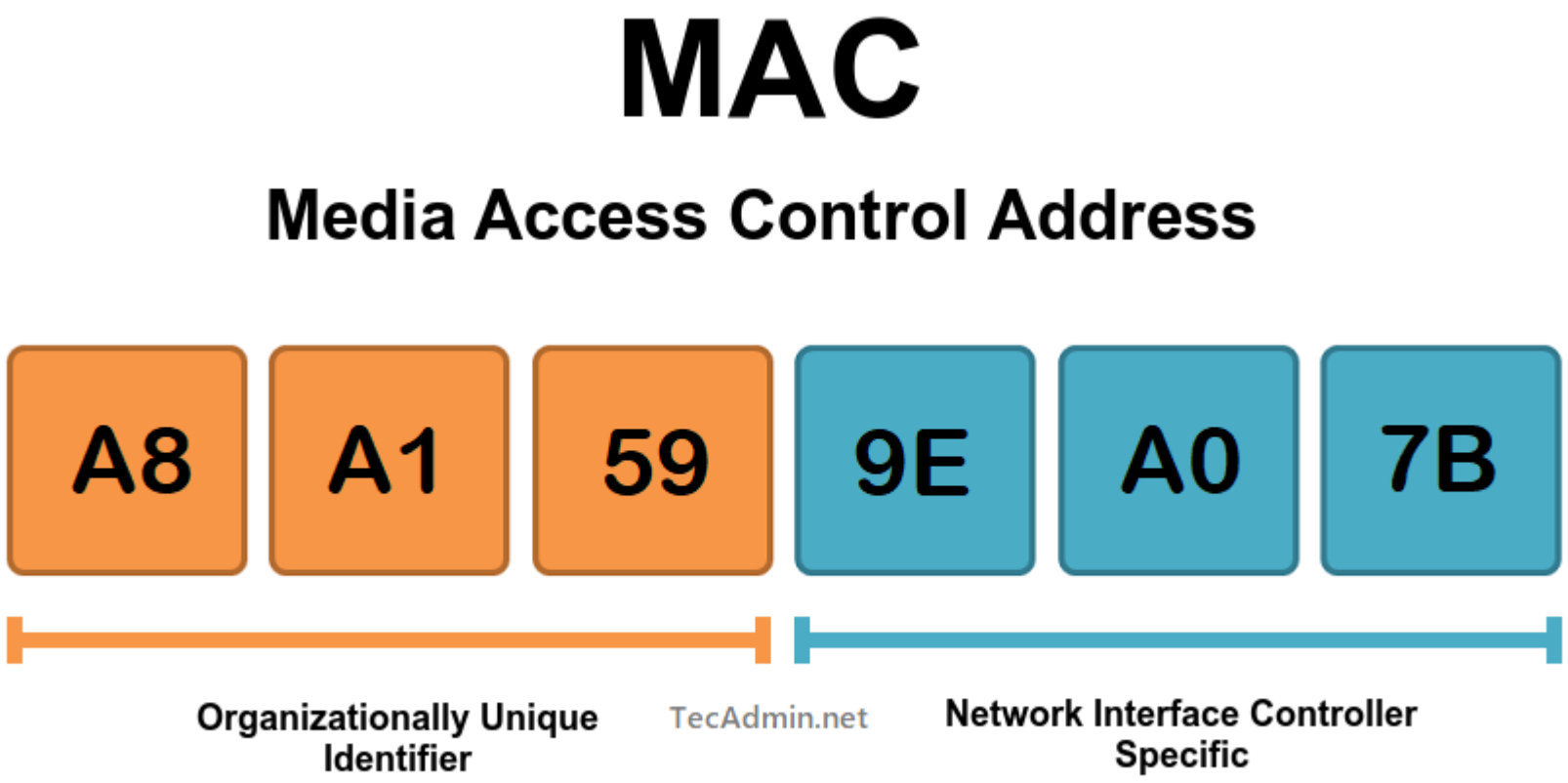
PUBLIC VS PRIVATE IP ADDRESSES



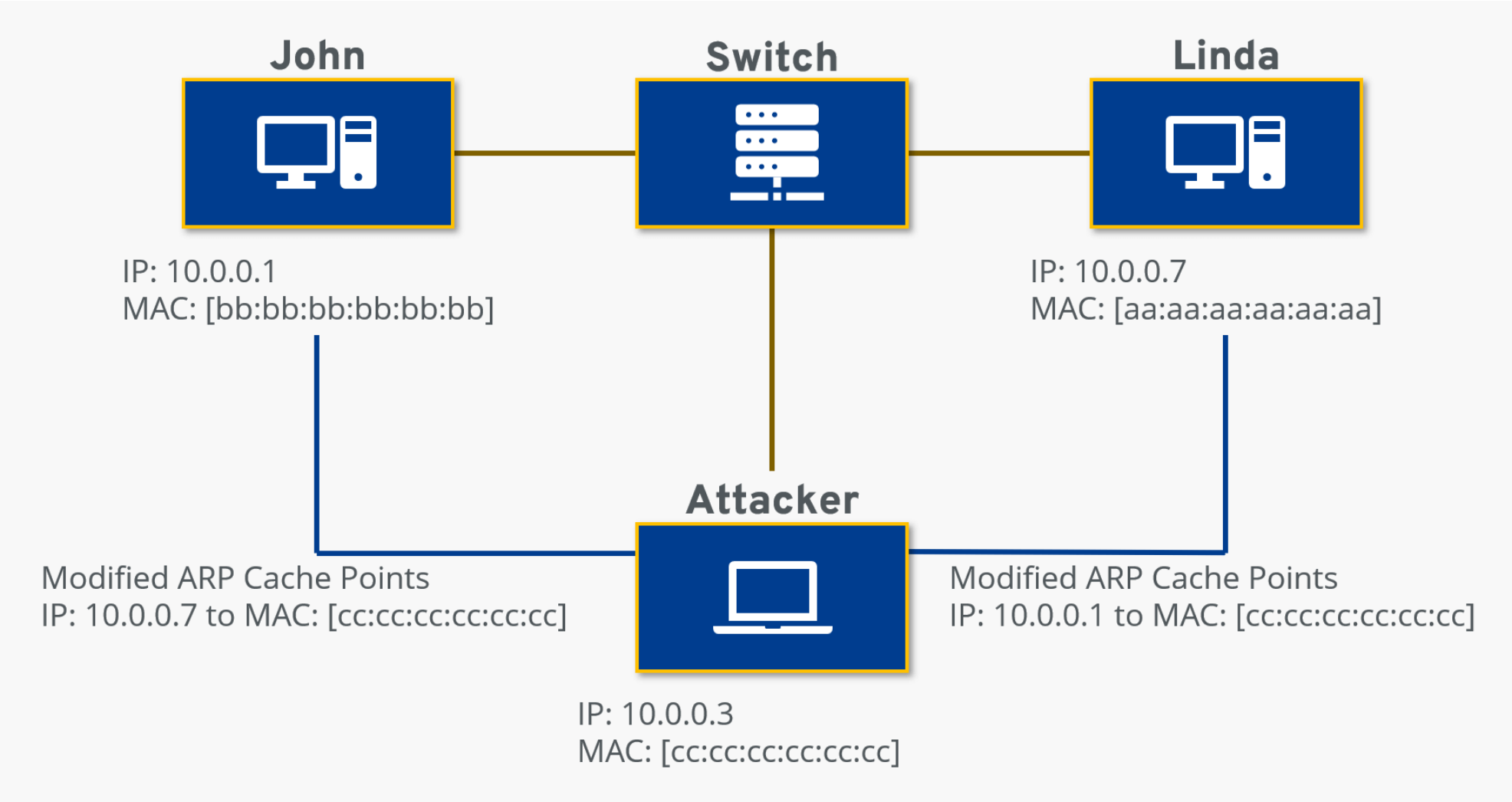
NETWORK ADDRESS TRANSLATION (NAT)



MAC ADDRESSES



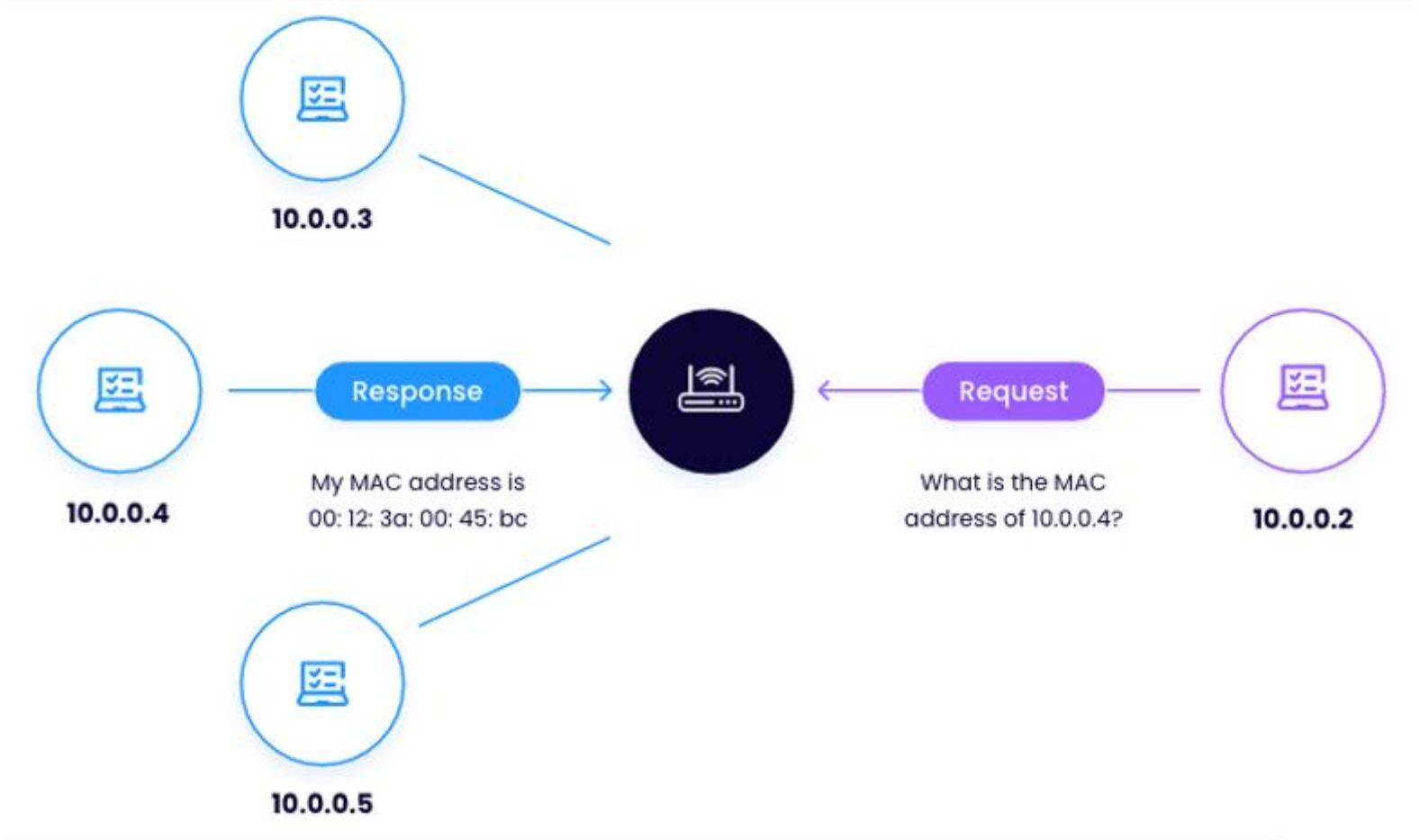
THE ARP SPOOFING ATTACKS



THE ARP SPOOFING ATTACKS

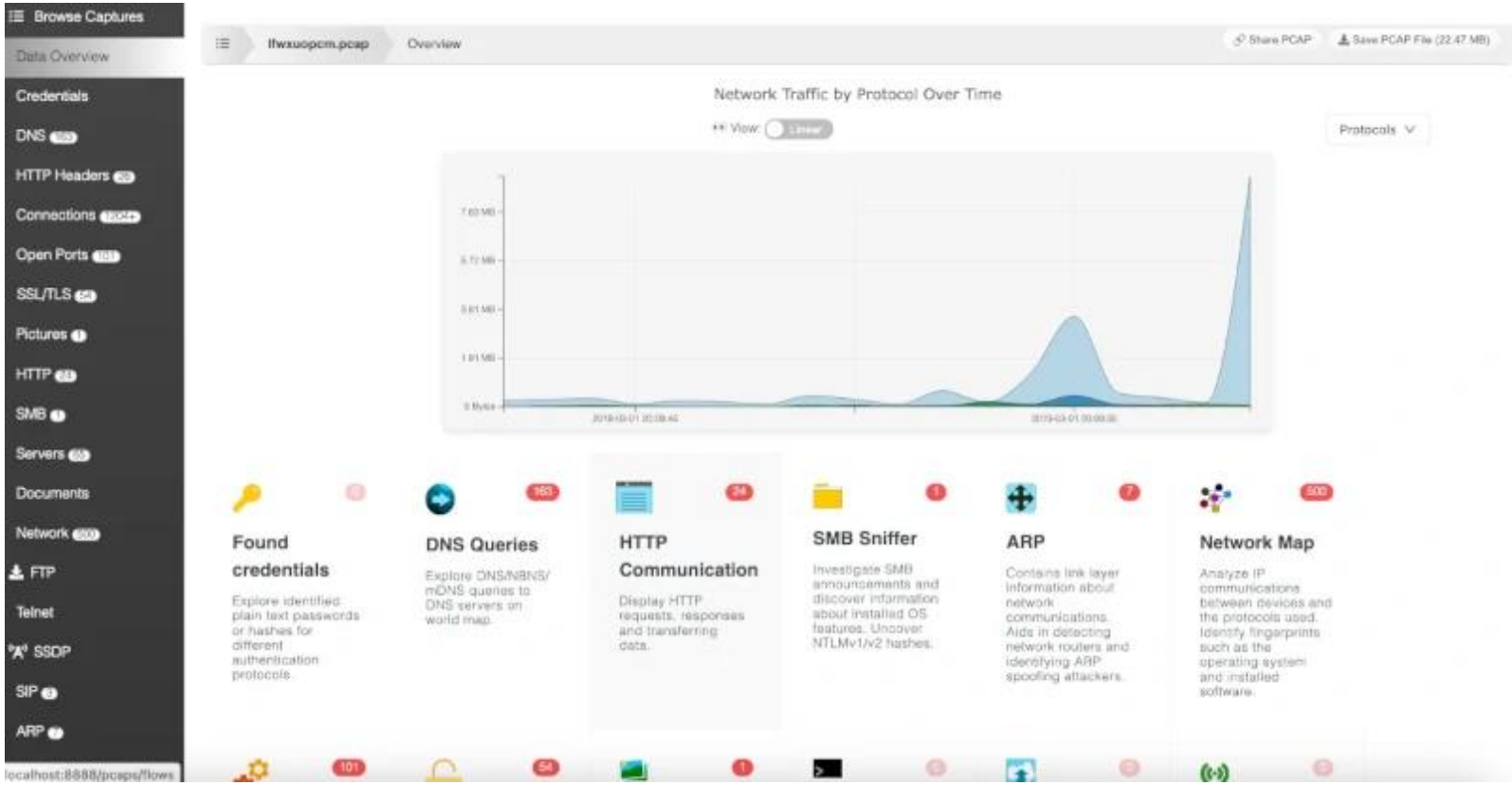
- **Practice:**
- ❑ **Eavesdropping**
- ❑ **MITM**
- ❑ **Denial of Service**

ARP SPOOFING ANALYSIS WITH WIRESHARK

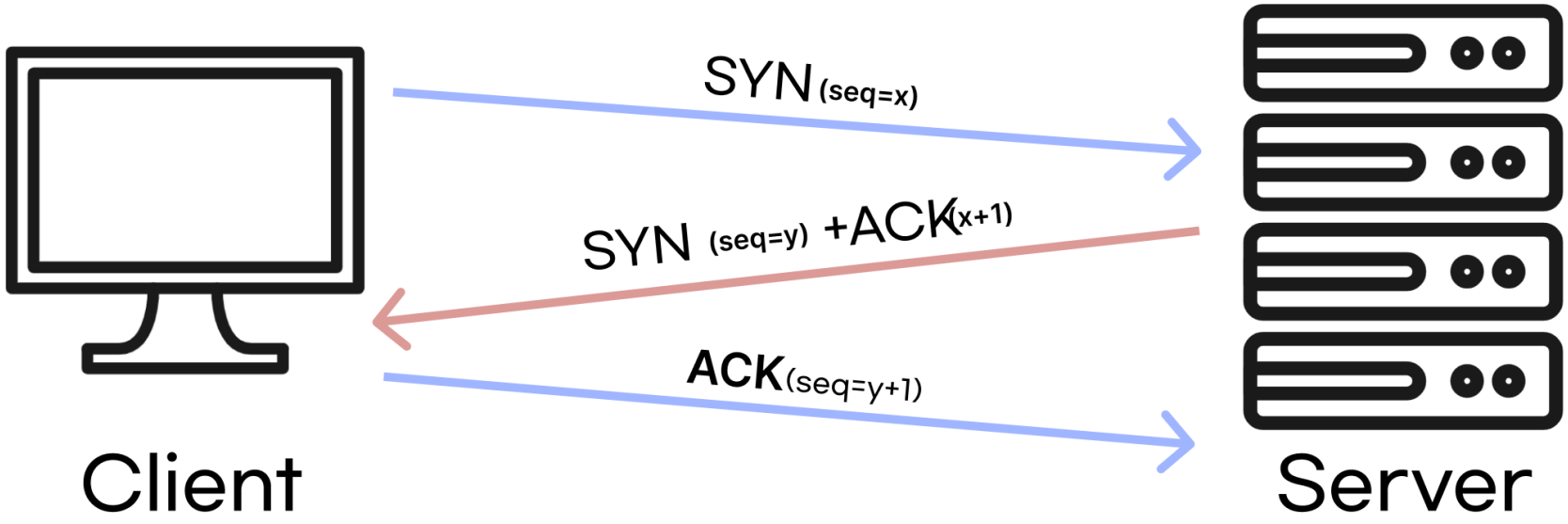


PACKET FLOW AND PACKET ANALYSIS

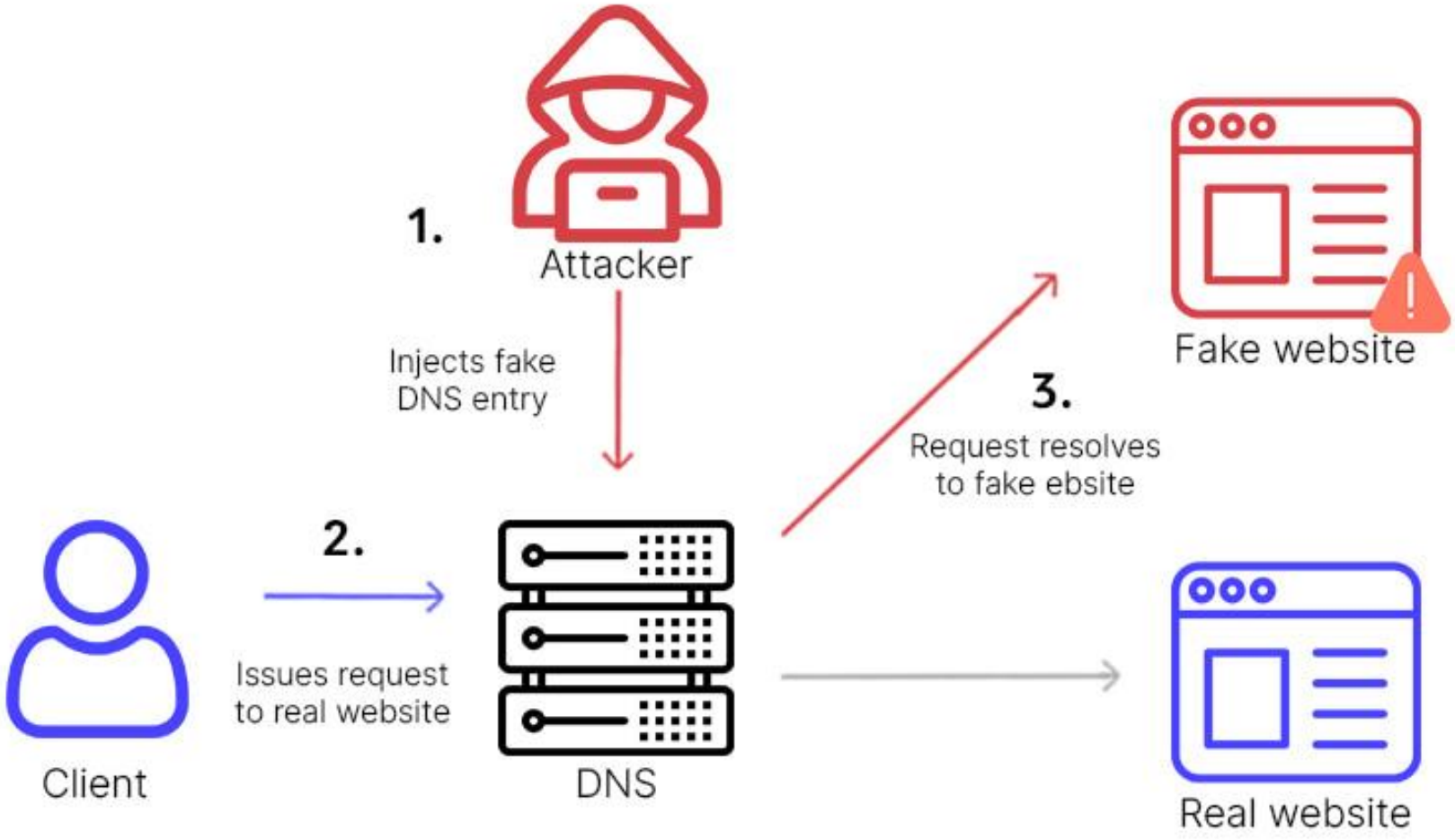
- **apackets.com**



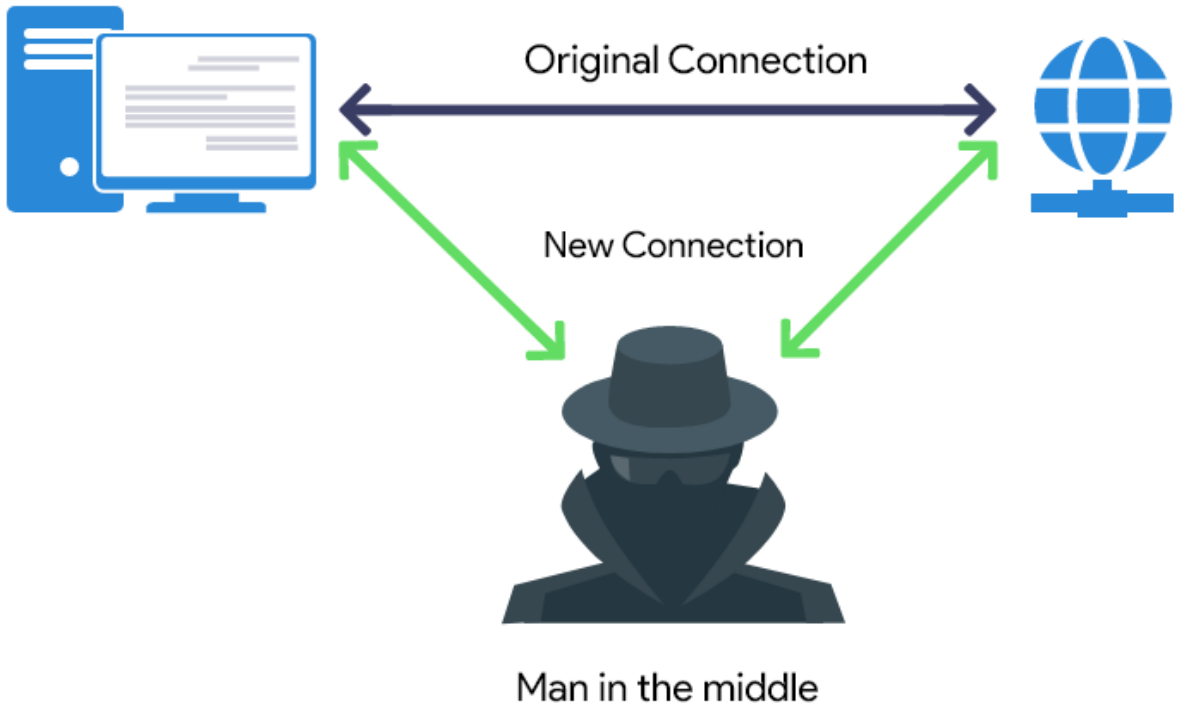
PRACTICAL ANALYSIS OF TCP THREE-WAY HANDSHAKE



DNS SPOOFING ATTACK



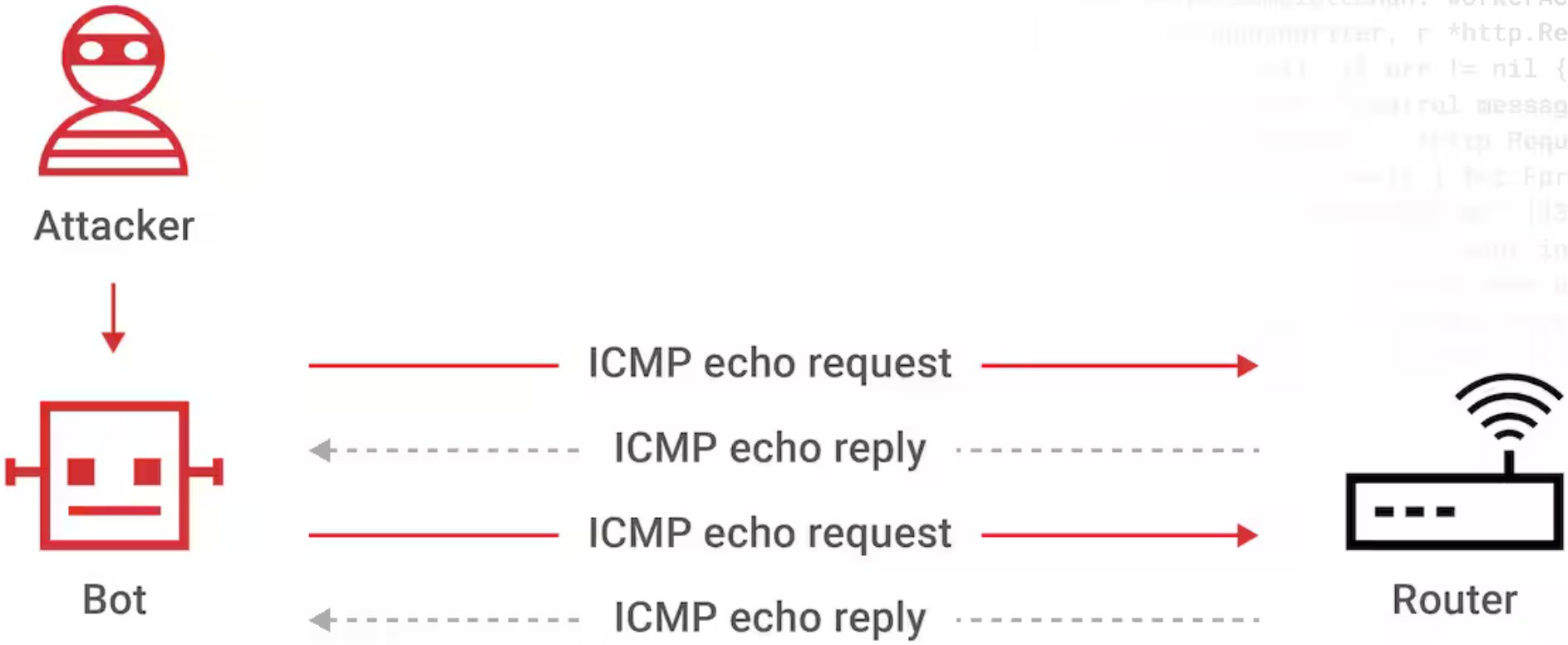
MAN IN THE MIDDLE ATTACK



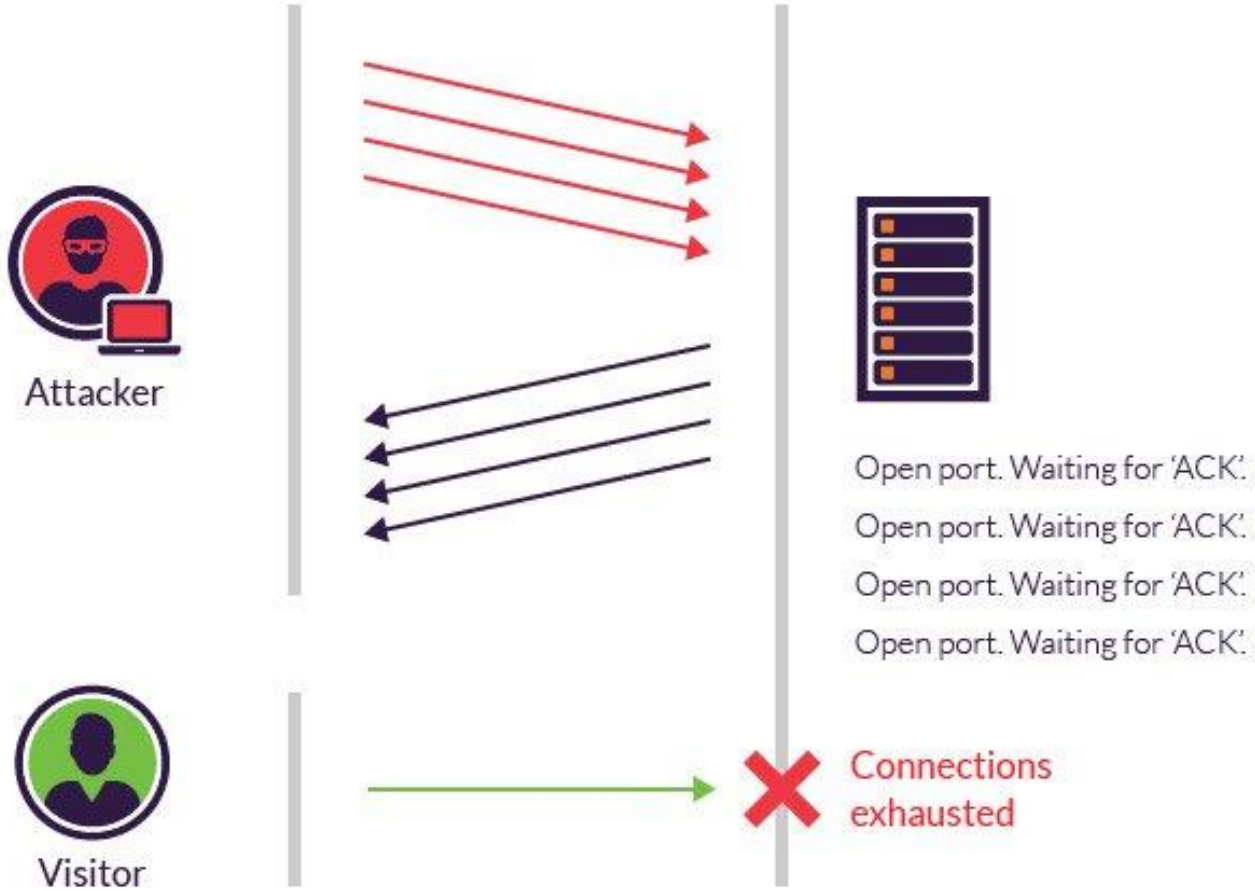
DOS & DDOS ATTACK

- Ping of Death attack
- Ping Flood Attack
- UDP Flood, TCP Flood Attack
- Smurf Attack

PING FLOOD ATTACK



TCP SYN FLOOD ATTACK



REFERENCES

- Cisco's Introduction to Cybersecurity
- mailtrap.io/blog/email-headers
- app.letsdefend.io/email-header-analysis
- Cybrary's Network Fundamentals Course
- Networking For Cybersecurity