# MALWARE TRAFFIC ANALYSIS

*Δημήτριος Τασιόπουλος*


# ΧΡΗΣΗ ΚΑΤΑΓΡΑΦΩΝ ΔΙΚΤΥΟΥ

## ΥΓΕΙΑ ΔΙΚΤΥΟΥ ΚΑΙ ΑΠΟΔΟΤΙΚΗ ΛΕΙΤΟΥΡΓΙΑ

- Βοηθούν τους μηχανικούς δικτύων να αναγνωρίσουν και να διαγνώσουν προβλήματα (latency, bottlenecks, faulty configurations)
- Υπολογισμός απόδοσης δικτύου (ταχύτητα, bandwidth, utilization)

## ΕΝΤΟΠΙΣΜΟΣ ΑΣΥΝΗΘΙΣΤΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ

Επιτρέπουν την ανίχνευση ύποπτης ή κακόβουλης δραστηριότητας (Intrusion Detection System, Firewall, Network Test Access Points)

## ΑΝΑΛΥΣΗ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

- Δυναμική ανάλυση
- Indicators of Compromise (IOC)

# CRASH COURSE 1

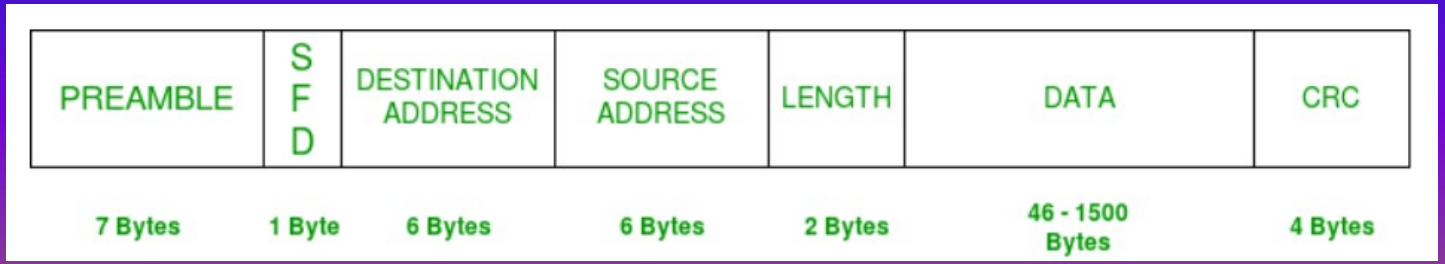
## ΠΡΩΤΟΚΟΛΛΑ

Physical Layer

- Υπεύθυνο για τη μετάδοση και λήψη δεδομένων μεταξύ συσκευών
- Raw data
- Ενσύρματες – Ασύρματες μεταδόσεις

Data Link Layer

- Υπεύθυνο για την αξιόπιστη και αποδοτική επικοινωνία μεταξύ δύο κόμβων του δικτύου
- Διευθύνσεις MAC
- Ethernet encapsulation - Frames



# CRASH COURSE 1

## ΠΡΩΤΟΚΟΛΛΑ

Network Layer

Υπεύθυνο για τη δρομολόγηση των πακέτων δεδομένων από τον αποστολέα στον παραλήπτη

πακέτο δεδομένων = μονάδα δεδομένων
IP protocol: Διευθυνσιοδότηση κόμβων

IPv4 ($2^{32}$ διευθύνσεις ~= 4 δις)

Non-Routable addresses:
10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
192.168.0.0 to 192.168.255.255

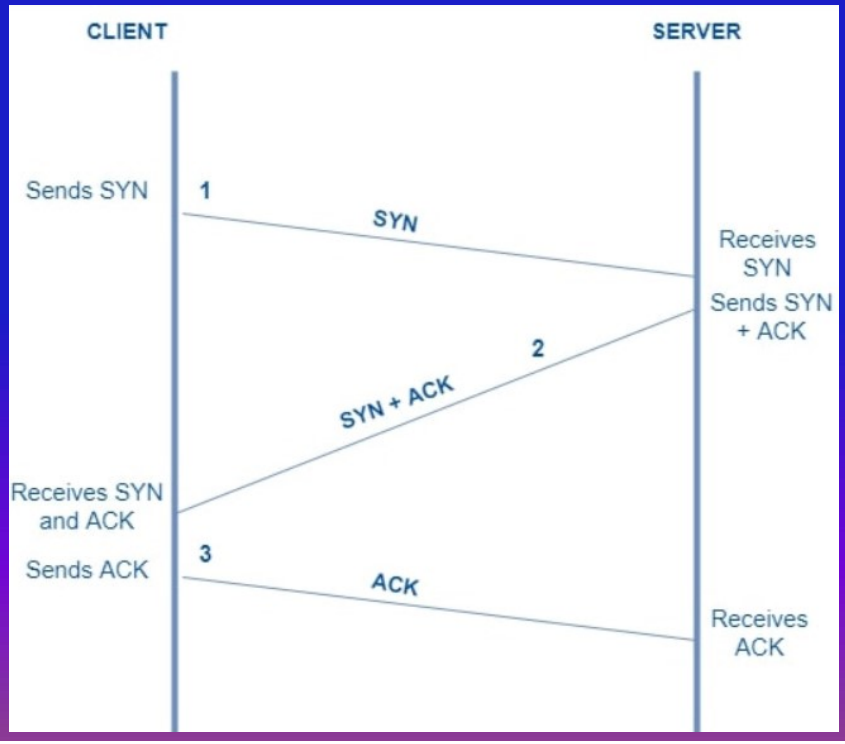
IPv6 ($2^{128}$ διευθύνσεις)

# CRASH COURSE 1

# ΠΡΩΤΟΚΟΛΛΑ

Transport Layer

- TCP
  - Connection – oriented (reliable, ordered, error-checked)
  - TCP segment
  - Ports

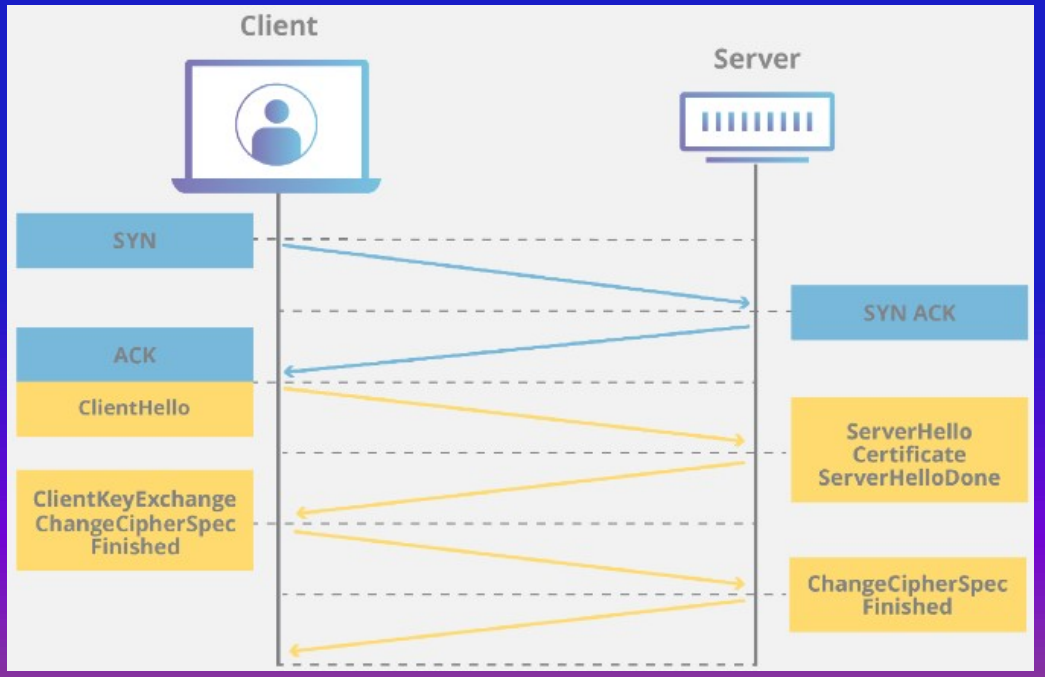


# CRASH COURSE 1

# ΠΡΩΤΟΚΟΛΛΑ

Transport Layer

TLS (Πρωτόκολλο κρυπτογράφησης επικοινωνιών)
Public Key Encryption
Certificates

# CRASH COURSE 1

# ΠΡΩΤΟΚΟΛΛΑ

Application Layer

HTTP

*http://www....*

stateless

request – response model

```
HTTP/1.1 200 OK
Date: Mon, 23 May 2005 22:38:34 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 155
Last-Modified: Wed, 08 Jan 2003 23:11:55 GMT
Server: Apache/1.3.3.7 (Unix) (Red-Hat/Linux)
ETag: "3f80f-1b6-3e1cb03b"
Accept-Ranges: bytes
Connection: close

<html>
  <head>
    <title>An Example Page</title>
  </head>
  <body>
    <p>Hello World, this is a very simple HTML document.</p>
  </body>
</html>
```

```
GET / HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

# CRASH COURSE 1

## ΠΡΩΤΟΚΟΛΛΑ

Application Layer

DNS

Phonebook of the Internet **ds.uth.gr** → **194.177.200.8**

Active Directory (AD)

Σύνολο υπηρεσιών + Βάσης Δεδομένων των Windows για τη διαχείριση των πόρων του δικτύου

LDAP

Επικοινωνία των υπηρεσιών του (AD)

Kerberos

Πρωτόκολλο Αυθεντικοποίησης σε περιβάλλον (AD)

Authentication Server - Ticket-Granting Server - Key Distribution Server

# CRASH COURSE 2

# FILE HASH

Συναρτήσεις Κατακερματισμού

Ψηφιακό «δαχτυλικό αποτύπωμα»

Εξασφαλίζει τη γνησιότητα ενός αρχείου


Empowering Teachers to Trigger **C**ybersecurity at School → SHA256

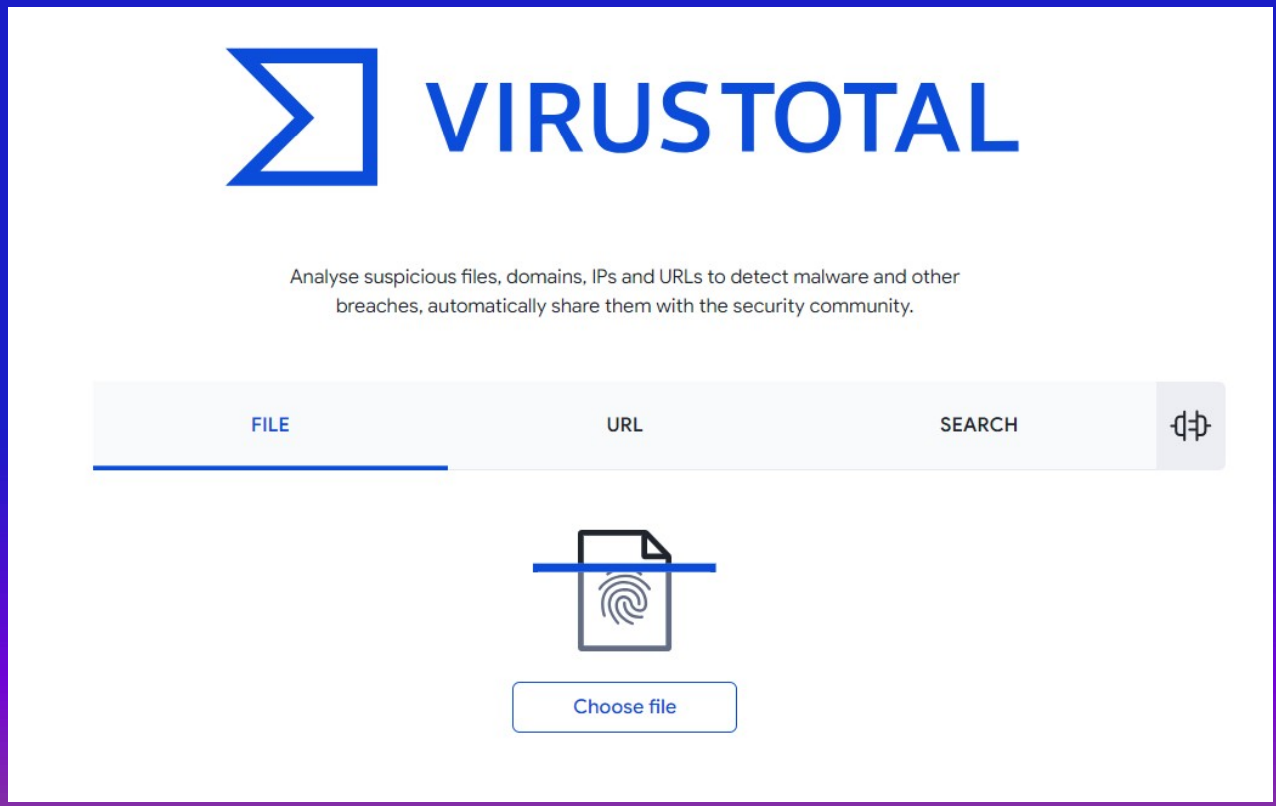
150f4ea7be888a4a9d70ddbb1ebd5ab04d2551edaa2f384825746ec764f812b3

Empowering Teachers to Trigger **c**ybersecurity at School → SHA256

ff8adff9c37dc4abc33dc2cfe2dc241b574bdabf5858343bc71bde3a34d8c36e

# CRASH COURSE 2

# OSINT ΕΡΓΑΛΕΙΑ



# CRASH COURSE 2

# OSINT ΕΡΓΑΛΕΙΑ

## URLhaus Database

Here you can propose new malware urls or just browse the URLhaus database. If you are looking for a parsable list of the dataset, you might want to check out the URLhaus API.

There are **2'689'001** malicious URLs tracked on URLhaus. The queue size is **0**.

## Submit a URL

In order to submit a URL to URLhaus, you need to login with your abuse.ch account

## Browse Database

domain, url, md5, sha256, tag:SocGholish, filetype:doc or url_status:online

Search

| Dateadded (UTC) | Malware URL | Status | Tags | Reporter |
|---|---|---|---|---|
| 2023-11-03 08:18:08 | http://220.87.49.57:43941/bin.sh | Online | 32-bit elf mips Mozi | geenensp |

# MALWARE TRAFFIC ACTIVITY

Λήψη κακόβουλου λογισμικού (staged approach)

Data Exfiltration

Beaconing (Command & Control Server)

Movement (Lateral / Vertical)

# WIRESHARK

Περιβάλλον

Ανάλυση αρχείου καταγραφής

- Initial infection
- Post – Infection activity