



RECOLECCION SEMI PASIVA DE INFORMACION

FOCA

1. Virtualizar el SO de un Windows 10

2. Ya virtualizado descargar FOCA

Google

A search bar with the query "foca elevenpath site:github.com".

X



Buscar con Google

Voy a tener suerte

Ofrecido por Google en: català galego euskara English



github.com › ElevenPaths › FOCA ▾ Traducir esta página

[ElevenPaths/FOCA: Tool to find metadata and hidden ... - Git...](#)

FOCA (Fingerprinting Organizations with Collected Archives). FOCA is a tool used mainly to find metadata and hidden information in the documents it scans.

[ElevenPaths/FOCA · GitHub](#) · Issues 3 · Projects 0

3. Ir a releases y descargar la ultima versión

iobyte Fixes bug on delete file (#100) c2b11a3 on Apr 15, 2020 85 commits

FOCA	Fixes bug on delete file (#100)	9 months ago
MetadataExtractCore	Clean references and update packages (#99)	10 months ago
Plugin example/FocaPluginExample	Clean unnecessary files	2 years ago
Plugins Release	Update.	3 years ago
PluginsAPI source	Clean unnecessary files	2 years ago
SearcherCore/SearcherCore	Clean references and update packages (#99)	10 months ago
doc	Added Twitter and Wikipedia links. Changed License for Licence (#79)	16 months ago
.gitignore	Clean unnecessary files	2 years ago
FOCA3_Pro.sln	Foca Open Source	3 years ago
LICENSE.txt	Update Readme.	3 years ago
README.md	Fixing readme typos (#80)	16 months ago

Tool to find metadata and hidden information in the documents.

[www.elevenpaths.com/es/labtools/fo...](#)

Readme

GPL-3.0 License

Releases 9

v3.4.7.0 Latest on Apr 3, 2020

+ 8 releases

Packages

No packages published

Contributors 8

Languages



4. Ir a google buscar y descargar sql server express 2022

Or, download a free specialized edition



Developer

SQL Server 2022 Developer is a full-featured free edition, licensed for use as a development and test database in a non-production environment.

[Download now](#)



Express

SQL Server 2022 Express is a free edition of SQL Server, ideal for development and production for desktop, web, and small server applications.

[Download now](#)



SQL SERVER 2022

Express Edition

Seleccione un tipo de instalación:

Básica

Seleccione el tipo de instalación Básica para instalar la funcionalidad de motor de base de datos de SQL Server con la configuración predeterminada.

Personalizado

Seleccione el tipo de instalación Personalizada para ejecutar paso a paso el asistente para instalación de SQL Server y elija los elementos que quiera instalar. Este tipo de instalación es detallado y lleva más tiempo que la instalación Básica.

Descargar medios

Descargue los archivos de instalación de SQL Server ahora e instálelos más tarde en una máquina de su elección.

5. Luego de esto extraer la información de la carpeta FOCA y ejecutar el programa

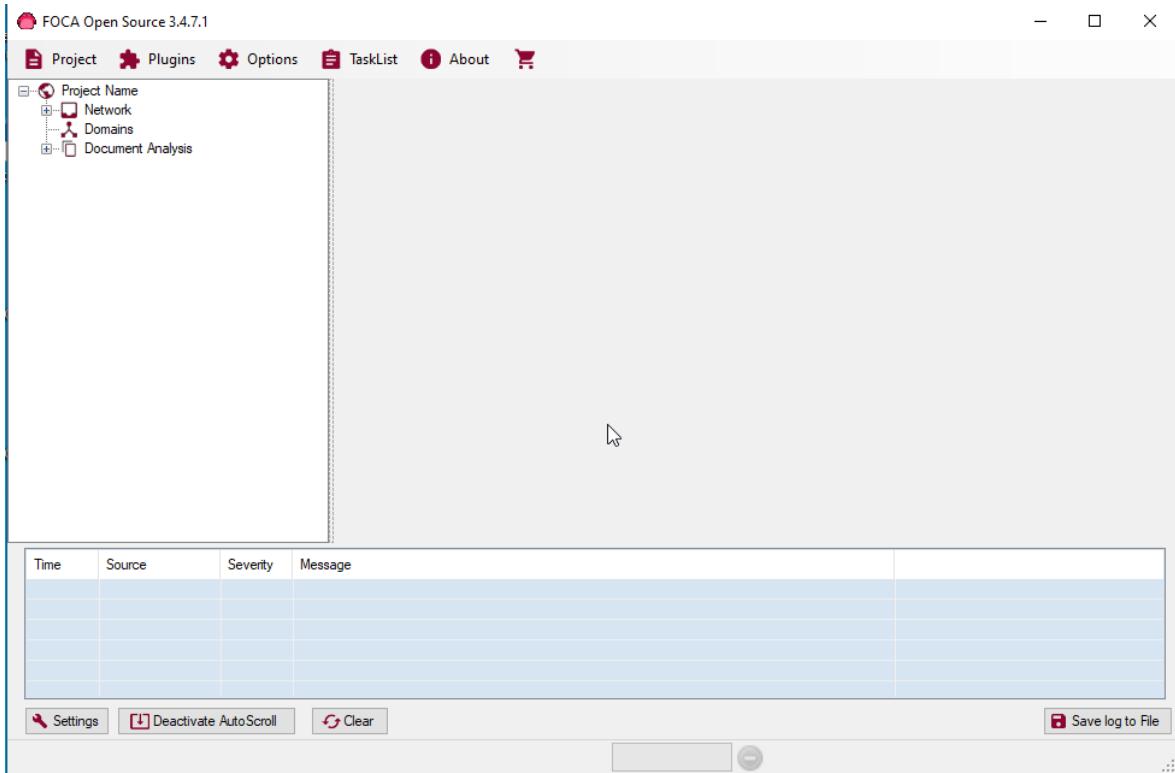


FOCA-v3.4.7.1			
Archivo	Inicio	Compartir	Vista
Herramientas de aplicación		Buscar en FOCA-v3.4.7.1	
Acceso rápido	Nombre	Fecha de modificación	Tipo
Escritorio	BaseSDK.dll	11/09/2023 6:30 p. m.	Extensión de la
Descargas	com.rusanu.dataconnectiondialog.dll	11/09/2023 6:30 p. m.	Extensión de la
Documentos	DiarioSDKNet.dll	11/09/2023 6:30 p. m.	Extensión de la
Imágenes	DotNetZip.dll	11/09/2023 6:30 p. m.	Extensión de la
Música	EntityFramework.dll	11/09/2023 6:30 p. m.	Extensión de la
Vídeos	EntityFramework.SqlServer.dll	11/09/2023 6:30 p. m.	Extensión de la
OneDrive	FOCA	11/09/2023 6:30 p. m.	Aplicación
Este equipo	FOCA.exe.config	11/09/2023 6:30 p. m.	Archivo CONFIG
Red	Google.Apis.Core.dll	11/09/2023 6:30 p. m.	Extensión de la
	Google.Apis.Customsearch.v1.dll	11/09/2023 6:30 p. m.	Extensión de la
	Google.Apis.dll	11/09/2023 6:30 p. m.	Extensión de la
	Google.Apis.PlatformServices.dll	11/09/2023 6:30 p. m.	Extensión de la
	Heijden.Dns.dll	11/09/2023 6:30 p. m.	Extensión de la
	HtmlAgilityPack.dll	11/09/2023 6:30 p. m.	Extensión de la
	MetadataExtractCore.dll	11/09/2023 6:30 p. m.	Extensión de la
	MetadataExtractor.dll	11/09/2023 6:30 p. m.	Extensión de la
	Newtonsoft.Json.dll	11/09/2023 6:30 p. m.	Extensión de la
	NLog.dll	11/09/2023 6:30 p. m.	Extensión de la
	ParallelExtensionsExtras.dll	11/09/2023 6:30 p. m.	Extensión de la
	PdfSharp.Charting.dll	11/09/2023 6:30 p. m.	Extensión de la
	PDFsharp.dll	11/09/2023 6:30 p. m.	Extensión de la
33 elementos 1 elemento seleccionado 2,54 MB			

FOCA-v3.4.7.1			
Archivo	Inicio	Compartir	Vista
Herramientas de aplicación		Buscar en FOCA-v3.4.7.1	
Acceso rápido	Nombre	Fecha de modificación	Tipo
Escritorio	DotNetZip.dll	11/09/2023 6:30 p. m.	Extensión de la
Descargas	EntityFramework.dll	11/09/2023 6:30 p. m.	Extensión de la
Documentos	EntityFramework.SqlServer.dll	11/09/2023 6:30 p. m.	Extensión de la
Imágenes	FOCA	11/09/2023 6:30 p. m.	Aplicación
Música	FOCA.exe.config	11/09/2023 6:30 p. m.	Archivo CONFIG
Vídeos	Google.Apis.Core.dll	11/09/2023 6:30 p. m.	Extensión de la
OneDrive	Google.Apis.Customsearch.v1.dll	11/09/2023 6:30 p. m.	Extensión de la
Este equipo	Google.Apis.dll	11/09/2023 6:30 p. m.	Extensión de la
Red	Heijden.Dns.dll	11/09/2023 6:30 p. m.	Extensión de la
	HtmlAgilityPack.dll	11/09/2023 6:30 p. m.	Extensión de la
	MetadataExtractCore.dll	11/09/2023 6:30 p. m.	Extensión de la
	MetadataExtractor.dll	11/09/2023 6:30 p. m.	Extensión de la
	Newtonsoft.Json.dll	11/09/2023 6:30 p. m.	Extensión de la
	NLog.dll	11/09/2023 6:30 p. m.	Extensión de la
	ParallelExtensionsExtras.dll	11/09/2023 6:30 p. m.	Extensión de la
	PdfSharp.Charting.dll	11/09/2023 6:30 p. m.	Extensión de la
	PDFsharp.dll	11/09/2023 6:30 p. m.	Extensión de la
3.4.7.1			



6. Bienvenido a FOCA



7. Descargar un fichero en Google para empezar a hacer una prueba sencilla de el uso de FOCA.



Google

site:ucundinamarca.edu.co ext:pdf



Buscar con Google

Voy a tener suerte

Nuevo: Capacítate para el mercado laboral con el Certificado en Ciberseguridad de Google

Este archivo tiene permisos limitados. Es posible que no tenga acceso a algunas caras.

Universidad de Cundinamarca
Fusagasuga

ACUERDO N°

"POR EL CUAL SE REGLAMENTA LA APLICACIÓN DE ALGUNOS ASPECTOS DEL DECRETO 1279 DE 2002 EN LA UNIVERSIDAD DE CUNDINAMARCA"

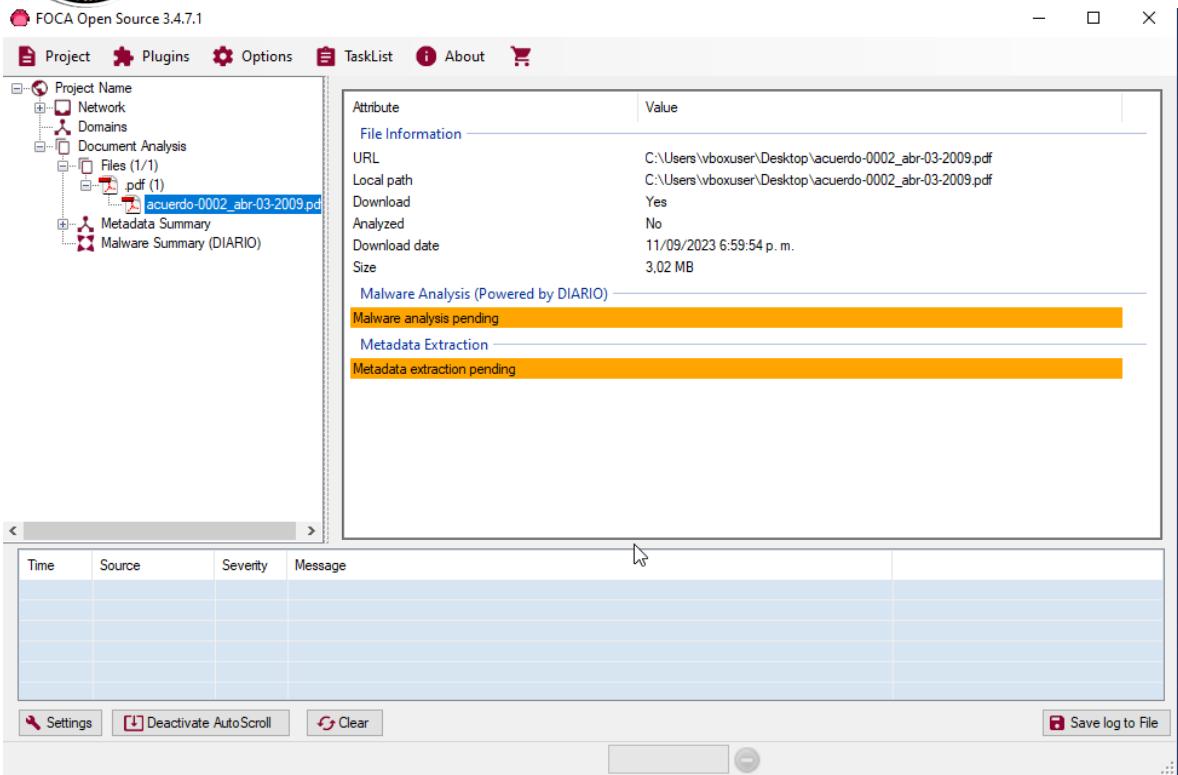
EL CONSEJO SUPERIOR DE LA UNIVERSIDAD DE CUNDINAMARCA, en uso de sus facultades legales y reglamentarias, en especial las conferidas por el artículo 10º del Acuerdo 010 de 2002 "Estatuto General" y por el Artículo 6º del Acuerdo 013 de 1996 "Estatuto Orgánico" de la Universidad de Cundinamarca y;

CONSIDERANDO

- Que mediante el Decreto 1279 de 2002, se estableció el régimen salarial y prestacional de los profesores de planta de las universidades estatales.
- Que el régimen salarial y prestacional contemplado en el Decreto 1279 determinó un sistema de puntos constitutivos de salario o de bonificación para los profesores de planta de las universidades estatales, en consideración, según el caso, a los títulos universitarios de pregrado o posgrado, la categoría en el escalafón docente, la productividad académica, las actividades de dirección académico-administrativas, la

8. Ir a Document Analysis y en el grafo dar clic derecho y add file





9. Como se evidencia no se ha realizado el análisis de metadata volvemos a document y extraemos la metadata



FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

Search engines: Google, Bing, DuckDuckGo

Project Name

- Network
- Domains
- Document Analysis
 - Files (1/1)
 - acuerdo-0002_abr-03-2009.pdf
- Metadata Summary
- Malware Summary (DIARIO)

Search All

Id Type URL Download Download Date Size Metadata

0	pdf	C:\Users\vhouser\Desktop\acuerdo-0002_abr-03-2009...	.	09/11/2023 18:59:54	3.02 MB	X
---	-----	--	---	---------------------	---------	---

Extract Metadata

- Download
- Extract Metadata
- Analyze Malware
- Delete
- Download All
- Extract All Metadata
- Analyze All Metadata
- Analyze All Malware
- Delete All
- Add file
- Add folder
- Add URLs from file
- Link(s)

Save log to File

Time Source Severity Message

Settings Deactivate AutoScroll Clear

FOCA Open Source 3.4.7.1

Project Plugins Options

Project Name

- Network
- Domains
- Document Analysis
 - Files (1/1)
 - acuerdo-0002_abr-03-2009.pdf
- Metadata Summary
 - Users (0)
 - Folders (0)
 - Printers (0)
 - Software (0)
 - Emails (0)
 - Operating Systems (0)
 - Passwords (0)
 - Servers (0)
- Malware Summary (DIARIO)



The screenshot shows the Maltego application interface. On the left, a tree view displays the project structure:

- Project Name
- Network
- Domains
- Document Analysis
 - Files (3/3)
 - pdf (2)
 - acuerdo-0002_abr-03-2009.pdf
 - R0371.pdf
 - Users
 - Dates
 - Software
 - Other Metadata
- Metadata Summary
 - Users (1)
 - Folders (0)
 - Printers (0)
 - Software (2) **(selected)**
 - Emails (0)
 - Operating Systems (0)
 - Passwords (0)
 - Servers (0)
- Malware Summary (DIARIO)

On the right, a summary panel titled "All software found (2) - Times found" lists the following data:

Attribute	Value
Software	PDF24 Creator
Software	GPL Ghostscript 9.27

10. Crearemos un proyecto para evitar la búsqueda uno a uno

The screenshot shows the FOCA Open Source 3.4.7.1 application window. The left sidebar displays a hierarchical tree view of the project structure:

- Project Name
- Network
- Domains
- Document Analysis
 - Files (3/3)
 - pdf (2)
 - acuerdo-0002_abr-03-2009.pdf
 - R0371.pdf
 - Users
 - Dates
 - Software
 - Other Metadata
- Metadata Summary
 - Users (1)
 - Folders (0)
 - Printers (0)
 - Software (2)
 - Emails (0)
 - Operating Systems (0)
 - Passwords (0)
 - Servers (0)
- Malware Summary (DIARIO)

The right panel contains two tables. The top table, titled "All software found (2) - Times found", lists software attributes and their values:

Attribute	Value
Software	PDF24 Creator
Software	GPL Ghostscript 9.27

The bottom table has columns for Time, Source, Severity, and Message, but no data is present.



TaskList About

Foca OPENSOURCE

Select project

Project name: Project of microsoft.com

Domain website: microsoft.com

Alternative domains:

Folder where to save documents: C:\Users\vboxuser\AppData\Local\Ti

Project date: lunes , 11 de septiembre de 2023

Project notes:

Create Import Cancel

Project of microsoft.com - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

Project of microsoft.com

- Network
- Domains
- Document Analysis

Foca
OPENSOURCE

Search engines: Google, Bing, DuckDuckGo

Extensions: All None

<input type="checkbox"/> doc	<input type="checkbox"/> docx	<input type="checkbox"/> sxw	<input type="checkbox"/> odp
<input type="checkbox"/> ppt	<input type="checkbox"/> pptx	<input type="checkbox"/> odt	<input type="checkbox"/> pdf
<input type="checkbox"/> pps	<input type="checkbox"/> ppss	<input type="checkbox"/> ods	<input type="checkbox"/> wpd
<input type="checkbox"/> xls	<input type="checkbox"/> xlss	<input type="checkbox"/> odg	<input type="checkbox"/> rtf

Custom search Search All

ID	Type	URL	Download	Download Date	Size	Metadata
Project of microsoft.com - FOCA Open Source 3.4.7.1						
Project saved successfully!						

Time Source Severity Message

Settings Deactivate AutoScroll Clear



Foca
OPENSOURCE

Custom search

Search engines Google Bing DuckDuckGo

Extensions All None

<input checked="" type="checkbox"/> doc	<input checked="" type="checkbox"/> docx	<input type="checkbox"/> sxw	<input type="checkbox"/> odp
<input checked="" type="checkbox"/> ppt	<input checked="" type="checkbox"/> ptx	<input type="checkbox"/> odt	<input checked="" type="checkbox"/> pdf
<input type="checkbox"/> pps	<input type="checkbox"/> ppsx	<input type="checkbox"/> ods	<input type="checkbox"/> wpd
<input type="checkbox"/> xls	<input checked="" type="checkbox"/> xlsx	<input checked="" type="checkbox"/> odg	<input type="checkbox"/> rtf

11. Seleccionar los resultados y hacer la extracción de metadata

Project of microsoft.com - FOCA Open Source 3.4.7.1

Project Plugins Options TaskList About

Project of microsoft.com Network Domains Document Analysis

Search engines Google Bing DuckDuckGo

Extensions All None

<input checked="" type="checkbox"/> doc	<input checked="" type="checkbox"/> docx	<input type="checkbox"/> sxw	<input type="checkbox"/> odp
<input checked="" type="checkbox"/> ppt	<input checked="" type="checkbox"/> ptx	<input type="checkbox"/> odt	<input checked="" type="checkbox"/> pdf
<input type="checkbox"/> pps	<input type="checkbox"/> ppsx	<input type="checkbox"/> ods	<input type="checkbox"/> wpd
<input type="checkbox"/> xls	<input checked="" type="checkbox"/> xlsx	<input checked="" type="checkbox"/> odg	<input type="checkbox"/> rtf

site:microsoft.c

ID	Type	URL	Download	Download Date	Size	Meta
27		https://queryprod.cms.it.microsoft.com/cms/api/am/bin...	X	-	23.06 KB	X
28	doc	https://download.microsoft.com/documents/customerevi...	X	-	505 KB	X
29	pdf	https://visualstudio.microsoft.com/wp-content/uploads/...	X	-	29.29 KB	X
30	doc	https://download.microsoft.com/documents/customerevi...	X	-	495.5 KB	X
31	doc	https://download.microsoft.com/documents/customerevi...	X	-	689.5 KB	X
32	doc	https://download.microsoft.com/documents/customerevi...	X	-	646.29 KB	X
33	pdf	https://adoption.microsoft.com/files/onedrive/OneDrive-...	X	-	506 KB	X
34	doc	https://download.microsoft.com/documents/customerevi...	X	-	520.5 KB	X
35	doc	https://download.microsoft.com/documents/customerevi...	X	-	443.5 KB	X
36	doc	https://download.microsoft.com/documents/customerevi...	X	-	-	X
37	pdf	https://news.microsoft.com/wp-content/uploads/prod/si...	X	-	-	X

Time Source Severity Message

7:14:57 ...	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 2
7:15:13 ...	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 0
7:15:35 ...	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 0
7:15:57 ...	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: Error en el servidor remoto: (403) Prohibido..
7:16:02 ...	MetadataSearch	medium	GoogleWeb search aborted!!

All searchers have finished



Foca
OPENSOURCE

Search engines: Google, Bing, DuckDuckGo

Extensions: All, None

Extension	doc	docx	sxw	odp
Extension	ppt	pptx	odt	pdf
Extension	pps	ppsx	ods	wpd
Extension	xls	xlsx	odg	rtf
Search engines	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Extensions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

site:microsoft.c)

Search All

ID	Type	URL	Download	Download Date	Size	Meta
27		https://query.prod.cms.rt.microsoft.com/cms/api/am/bin...	X	-	-	X
28	doc	https://download.microsoft.com/documents/customerevi...	•	09/11/2023 19:17:32	23.06 KB	X
29	pdf	https://visualstudio.microso...		09/11/2023 19:17:32	505 KB	X
30	doc	https://download.microso...		09/11/2023 19:17:32	29.29 KB	X
31	doc	https://download.microso...		-	495,5 KB	X
32	doc	https://download.microso...		-	689,5 KB	X
33	pdf	https://adoption.microso...		09/11/2023 19:17:33	646.29 KB	X
34	doc	https://download.microso...		-	506 KB	X
35	doc	https://download.microso...		-	520,5 KB	X
36	doc	https://download.microso...		-	443,5 KB	X
37	pdf	https://news.microsoft.com...		-	-	X

Right-click context menu for item 28:

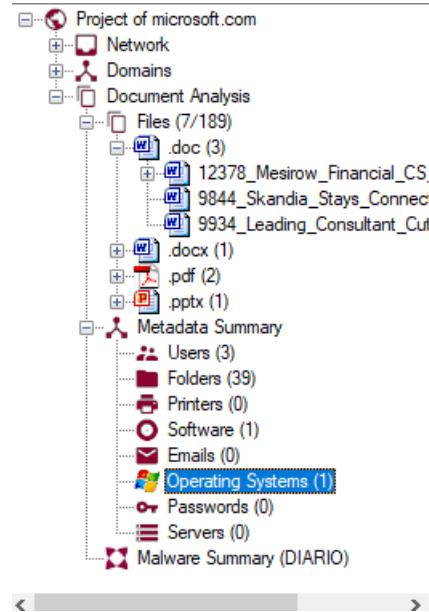
- Download
- Extract Metadata
- Analyze Malware
- Delete
- Download All
- Extract All Metadata
- Analyze All Metadata
- Analyze All Malware
- Delete All
- Add file
- Add folder
- Add URLs from file
- Link(s)

Log output:

```
Web search finished successfully!! Total found result
Web search finished successfully!! Total found result
Web search finished successfully!! Total found result
error has ocurred on DuckDuckGoWeb: Error en el se
singleWeb search aborted!!
```

Clear

Save log to File





METAGOOFIL

1. Actualizar el Kali con un

```
sudo apt-get update
```

```
kali㉿kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ sudo apt-get update
```

2. Instalamos el metagoofil

```
sudo apt-get install metagoofil
```

```
─(kali㉿kali)-[~]
$ sudo apt-get install metagoofil

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-googlesearch
The following NEW packages will be installed:
  metagoofil python3-googlesearch
0 upgraded, 2 newly installed, 0 to remove and 451 not upgraded.
Need to get 60.5 kB of archives.
After this operation, 208 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 python3-googlesearch all 2.0.3-0kali1 [45.1 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 metagoofil all 1:1.2.0+git20221009-0kali1 [15.4 kB]
Fetched 60.5 kB in 1s (76.9 kB/s)
Selecting previously unselected package python3-googlesearch.
(Reading database ... 398533 files and directories currently installed.)
Preparing to unpack ... /python3-googlesearch_2.0.3-0kali1_all.deb ...
Unpacking python3-googlesearch (2.0.3-0kali1) ...
Selecting previously unselected package metagoofil.
Preparing to unpack ... /metagoofil_1%3a1.2.0+git20221009-0kali1_all.deb ...
Unpacking metagoofil (1:1.2.0+git20221009-0kali1) ...
Setting up python3-googlesearch (2.0.3-0kali1) ...
```



3. metagoofil -h

```
(kali㉿kali)-[~]
$ metagoofil -h
usage: metagoofil.py [-h] -d DOMAIN [-e DELAY] [-f [SAVE_FILE]]
                      [-i URL_TIMEOUT] [-l SEARCH_MAX]
                      [-n DOWNLOAD_FILE_LIMIT] [-o SAVE_DIRECTORY]
                      [-r NUMBER_OF_THREADS] -t FILE_TYPES [-u [USER_AGENT]]
                      [-w]

Metagoofil v1.2.0 - Search Google and download specific file types.

options:
  -h, --help            show this help message and exit
  -d DOMAIN             Domain to search.
  -e DELAY              Delay (in seconds) between searches. If it's too
                        small Google may block your IP, too big and your
                        search may take a while. Default: 30.0
  -f [SAVE_FILE]         Save the html links to a file.
                        no -f = Do not save links
                        -f = Save links to html_links_<TIMESTAMP>.txt
                        -f SAVE_FILE = Save links to SAVE_FILE
  -i URL_TIMEOUT        Number of seconds to wait before timeout for
                        unreachable/stale pages. Default: 15
  -l SEARCH_MAX          Maximum results to search. Default: 100
  -n DOWNLOAD_FILE_LIMIT
                        Maximum number of files to download per filetype.
                        Default: 100
  -o SAVE_DIRECTORY      Directory to save downloaded files. Default is
                        current working directory, "."
  -r NUMBER_OF_THREADS   Number of downloader threads. Default: 8
  -t FILE_TYPES          file_types to download
                        (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx). To search
                        all 17,576 three-letter file extensions, type "ALL"
  -u [USER_AGENT]        User-Agent for file retrieval against -d domain.
                        no -u = "Mozilla/5.0 (compatible; Googlebot/2.1; +htt
p://www.google.com/bot.html)"
                        -u = Randomize User-Agent
                        -u "My custom user agent 2.0" = Your customized User-
Agent
  -w                     Download the files, instead of just viewing search
                        results.
```

metagoofil -d microsoft.com -l 10 -t pdf,doc,ppt -o Desktop

```
(kali㉿kali)-[~]
$ metagoofil -d microsoft.com -l 10 -t pdf,doc,ppt -o Desktop
[*] Searching for 10 .pdf files and waiting 30.0 seconds between searches
```

4. para poder ver los metadatos hay que insalar una utilidad



```
sudo apt-get imnstall exiftool
```

```
(kali㉿kali)-[~]
$ sudo apt-get install exiftool

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'libimage-exiftool-perl' instead of 'exiftool'
libimage-exiftool-perl is already the newest version (12.65+dfsg-1).
libimage-exiftool-perl set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 451 not upgraded.
```

```
Exiftool -r *.pdf | egrep -i "Author|Creator|Email| Producer | Template" | sort -u
```



DNS DUMPSTER

The screenshot shows the dnsdumpster.com interface with the search term "exampledomain.com" entered. The results page displays two main sections: "Hosting (IP block owners)" and "GeoIP of Host Locations".

Hosting (IP block owners)

IP Block Owner	Count
AKAMAI-ASN2	2
MICROSOFT-CORP-MSNLAS-BLOCK	1
AKAMAI-ASN	1
TESLA	20
EFACT7	10
OTSI-SAC	5
SENDERO	3
AKAMAI-ASN1	1
CHINANET-SH4AP	1
GO-DADDY-COM-LLC	1
SOMERVILLE-AS-ALLAP	1
SIN Shanghai Information Network Co	1
CNNIC-DSNET-4AP	1
Shanghai Internet Co	1
ZAYO-4641	1

GeoIP of Host Locations

A world map where the United States is highlighted in green, indicating the geographical locations of the IP blocks associated with the domain tesla.com.

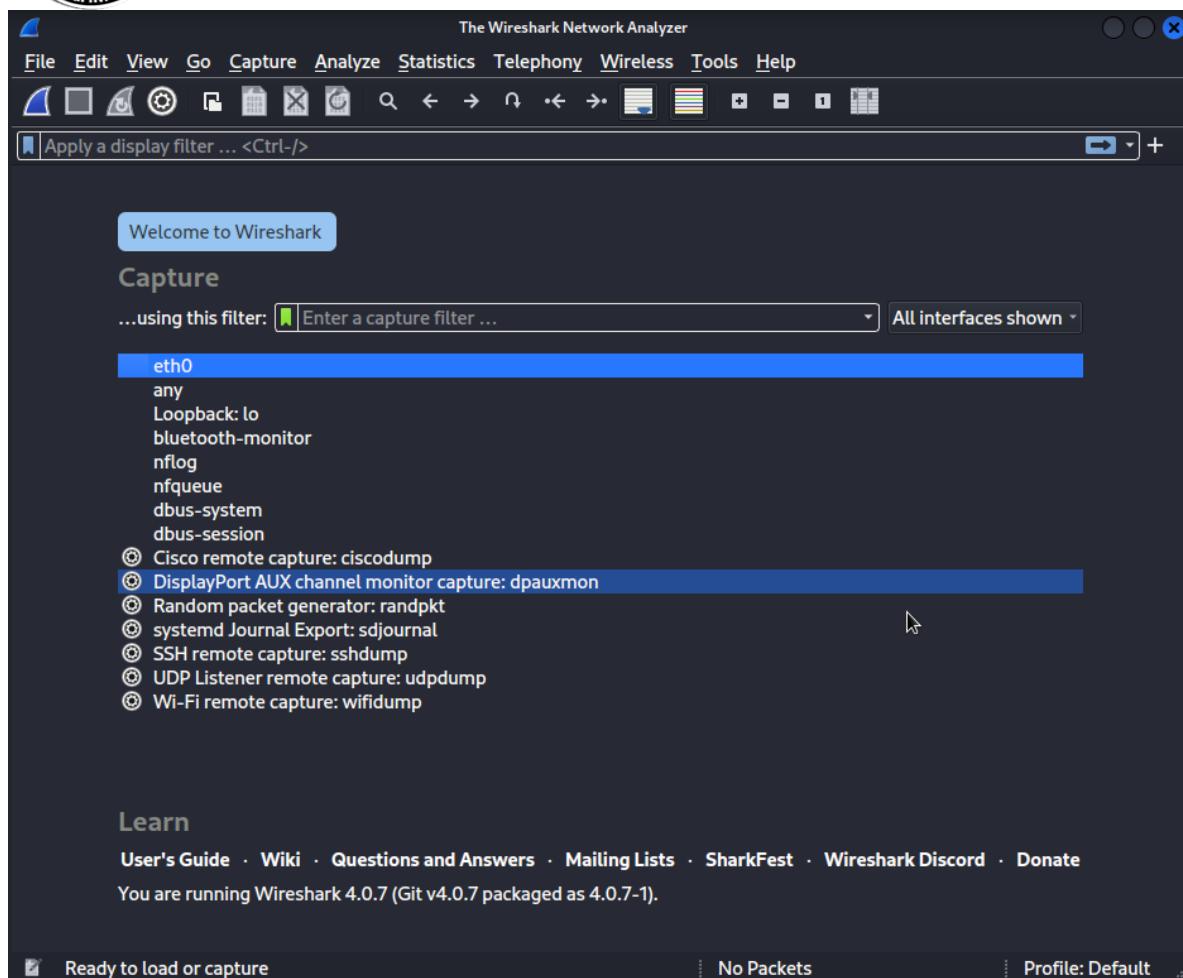


SNIFFERS:WIRESHARK

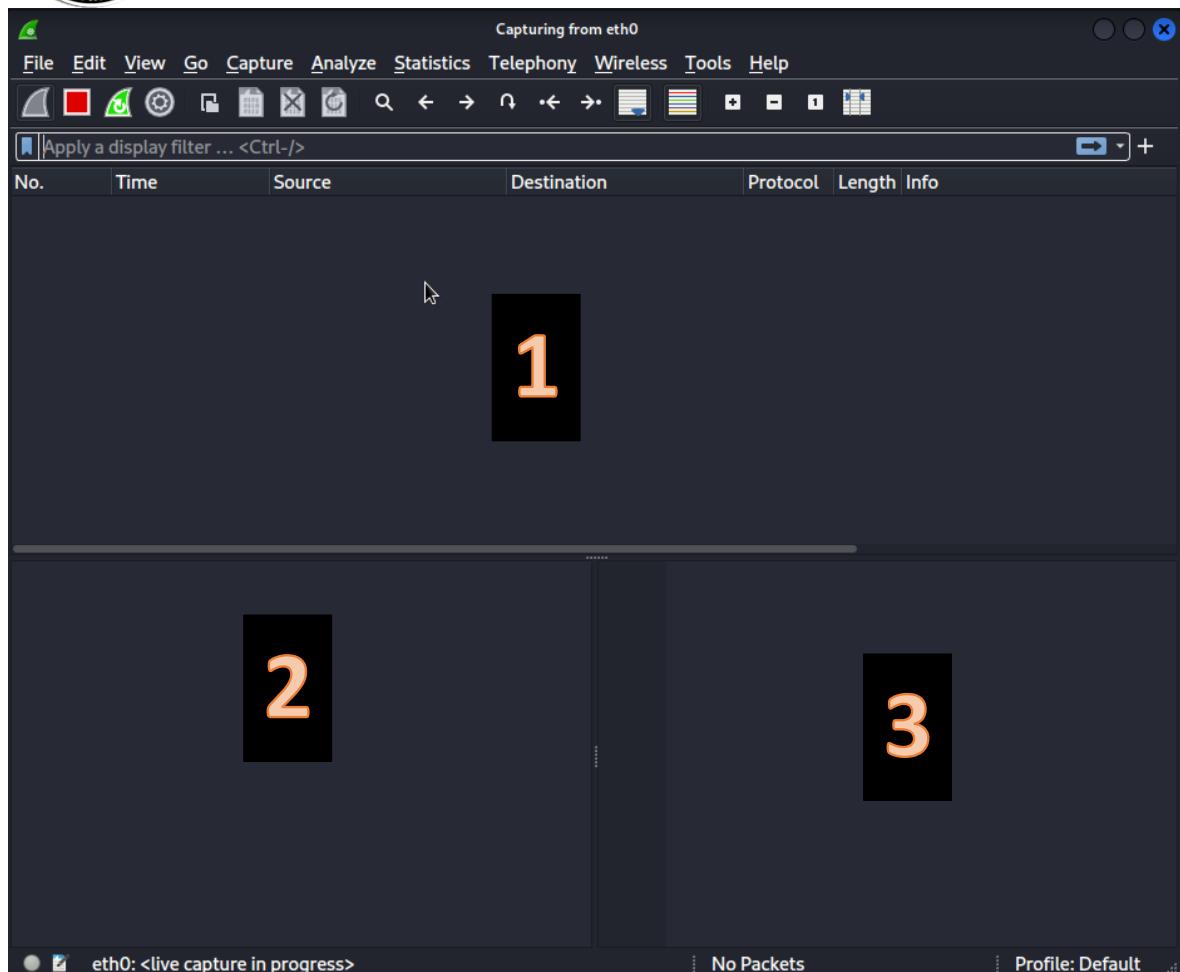
1. ingresar a wireshark



2. conociendo la interfaz



3. Dar doble clic en cualquier interfaz en este caso la que nos interesa es la eth0



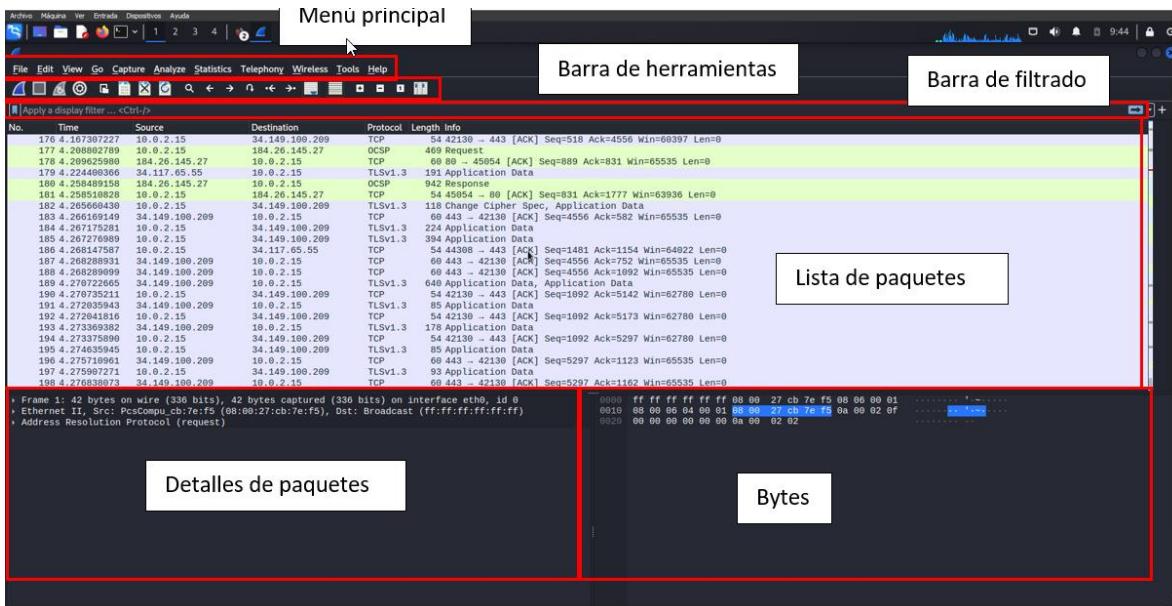
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No. Iniciar captura Detener captura Reiniciar captura

No.	Source	Destination	Protocol	Length	Info
81	192.168.1.157	10.0.2.15	QUIC	72	Protected Payload (KPO), DCID=09fbed
81	192.168.1.157	10.0.2.15	QUIC	204	Protected Payload (KPO), DCID=09fbed
81	192.168.1.157	10.0.2.15	QUIC	70	Protected Payload (KPO), DCID=09fbed
877 2.048321141	10.0.2.15	172.217.192.157	QUIC	78	Protected Payload (KPO), DCID=a663985590058d82
878 2.053583165	10.0.2.15	172.217.192.157	QUIC	295	Protected Payload (KPO), DCID=7889d7c1de061a28
879 2.067888631	142.251.0.157	10.0.2.15	QUIC	70	Protected Payload (KPO), DCID=3c1cd2
880 2.084589888	64.233.186.156	10.0.2.15	TLSv1.3	662	Application Data, Application Data
881 2.084611719	10.0.2.15	64.233.186.156	TCP	54	55396 → 443 [ACK] Seq=752 Ack=4914 Win=62780 Len=0
882 2.085316741	64.233.186.156	10.0.2.15	TLSv1.3	85	Application Data
883 2.085360683	10.0.2.15	64.233.186.156	TCP	54	55396 → 443 [ACK] Seq=752 Ack=4945 Win=62780 Len=0
884 2.085506416	10.0.2.15	64.233.186.156	TLSv1.3	85	Application Data
885 2.101771997	172.217.192.157	10.0.2.15	QUIC	72	Protected Payload (KPO), DCID=67492d
886 2.104024461	172.217.192.157	10.0.2.15	QUIC	104	Protected Payload (KPO), DCID=67492d
887 2.104025162	172.217.192.157	10.0.2.15	QUIC	70	Protected Payload (KPO), DCID=67492d
888 2.105219942	10.0.2.15	172.217.192.157	QUIC	78	Protected Payload (KPO), DCID=7889d7c1de061a28
889 2.121573195	172.217.192.157	10.0.2.15	QUIC	70	Protected Payload (KPO), DCID=09fbed
890 2.176489358	172.217.192.157	10.0.2.15	QUIC	70	Protected Payload (KPO), DCID=67492d
891 2.213454241	64.233.186.156	10.0.2.15	TCP	60	443 → 55396 [ACK] Seq=4945 Ack=783 Win=31986 Len=0

> Frame 277: 1399 bytes on wire (11192 bits), 1399 bytes captured (11192 bits) on interface eth0, id 0
> Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_95:bd:54 (08:00:27:95:bd:54)
> Internet Protocol Version 4, Src: 142.251.0.103, Dst: 10.0.2.15
> User Datagram Protocol, Src Port: 443, Dst Port: 45904
> QUIC IETF



4. General trafico de red



Archivo Máquina Ver Entrada Dispositivos Ayuda

1 2 3 4

Search bar

Favorites

Recently Used

All Applications

Settings

Usual Applications

01 - Information Gathering

02 - Vulnerability Analysis

03 - Web Application Analysis

04 - Database Assessment

05 - Password Attacks

06 - Wireless Attacks

07 - Reverse Engineering

08 - Exploitation Tools

09 - Sniffing & Spoofing

10 - Post Exploitation

11 - Forensics

12 - Reporting Tools

13 - Social Engineering Tools

42 - Kali & OffSec Links

Terminal Emulator

Root Terminal Emulator

File Manager

Text Editor

Web Browser

Kali Linux Browse the web

Kali Docs

Kali Bugs

OffSec Training

Exploit Database

VulnHub

Icons for each application: terminal, root terminal, file manager, text editor, browser, Kali Linux, Kali Docs, Kali Bugs, OffSec Training, Exploit Database, VulnHub.



Kali Linux

file:///usr/share/kali-def

Telephony Wireless Tools Help

Kali Linux Kali Tools Kali Docs Kali Forums

KALI

Want to know more about Kali? Search for it here.

Documentation Kali Tools

Check out what's new in the latest release of Kali Linux!

38 byt 0000 52 54 00 12 35 02 08 00 27 cb 7e f5 08
3:00:2 0010 00 4a da a8 40 00 40 11 2f 42 0a 00 02
2.15, 0020 64 01 e6 b8 00 35 00 36 31 00 13 a6 01
, Dst 0030 00 00 00 00 00 07 63 6f 6e 74 69 6c
0040 65 72 76 69 63 65 73 07 6d 6f 7a 69 6c
0050 63 6f 6d 00 00 01 00 01

Packets: 711 · Displayed: 711 (100.0%) · Profile: Default

The screenshot shows a Kali Linux desktop environment. On the left, a Firefox browser window displays the Kali Linux homepage. The main content area features the Kali Linux logo and navigation links for Documentation and Kali Tools. On the right, a NetworkMiner tool window is open, showing a list of network traffic entries. The interface includes tabs for Telephony, Wireless, Tools, and Help. The NetworkMiner table has columns for Destination, Protocol, Length, and Info. Below the table, there is a hex dump of network data. At the bottom of the NetworkMiner window, status information is displayed: Packets: 711 · Displayed: 711 (100.0%) · Profile: Default.

Ingresar a phrack.org



← → ⌂ https://phrack.org

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali Nethunter Exploit-DB Google Hacking DB

[News] [Issues] [Authors] [Archives] [Contact]

Phrack

::: Introduction :::

Issues	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]	[27]	[28]	[29]	[30]	[31]	[32]	[33]	[34]	[35]	[36]
[37]	[38]	[39]	[40]	[41]	[42]	[43]	[44]	[45]	[46]	[47]	[48]	[49]	[50]	[51]	[52]	[53]	[54]	[55]	[56]	[57]	[58]	[59]	[60]	[61]	[62]	[63]	[64]	[65]	[66]	[67]	[68]	[69]	[70]	[71]	[72]	

Current Issue : [72] | Release date : date: 2025-08-19 | Editor: author: Phrack Staff | Get tar.gz

Introduction Phrack Staff

Phrack Prophele on Gera Phrack Staff

Linenuse Phrack Staff

Loopback Phrack Staff

The Art of PHP - My CTF Journey and Untold Stories! Orange Thr

Guarding the PHP Temple m7_my

JPN Devs Re-implement Kurea Rets Saber, CV000

Aarming reimplementation CVE-2020-9273 shakir

Mapping ZXCS Metrics Exposed to User Space on macOS Kent Madsen

Popping an alert from a sandboxed WebAssembly module Thomas Blomk

Decrypt the Planes - Rayne RCE Simon, Pedro, Jason

Quantum ROP Yosef Shiffman, Yehav Raham

Revisiting Similarities of Android Apps Jakob Blaer, Martina Lindner

Money for Nothing, Chips for Free Peter Honeyman

E0 - Selective Symbolic Instrumentation jek Amy

Roadside to Everyone Jon Gaines

A CPU Backdoor u7y

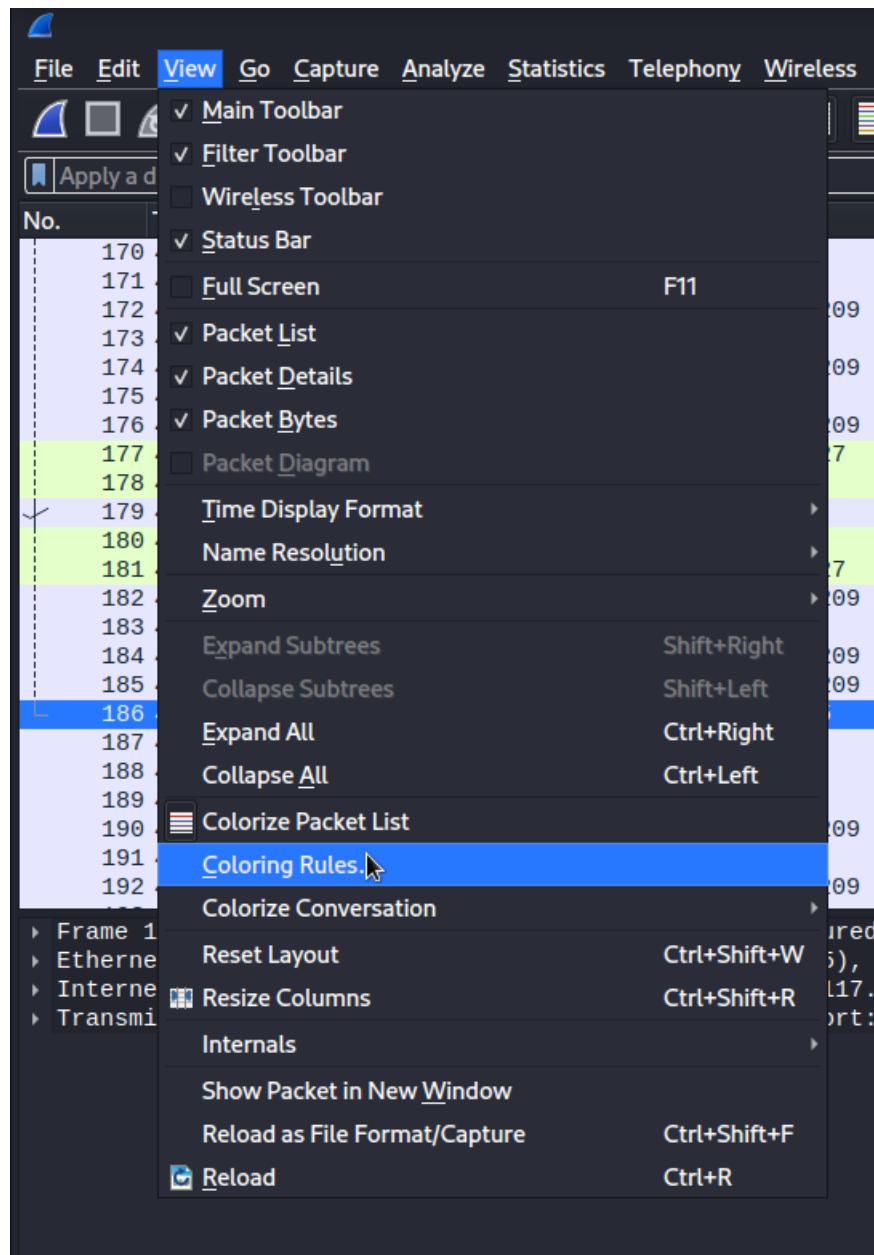
The Feed Is Ours tgr

The Hacker's Renaissance - A Manifesto Reborn TH2

Title: Introduction

Author: Phrack Staff

[View as text](#)





Wireshark - Coloring Rules Default

Name	Filter
Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
HSRP State Change	hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change	stp.type == 0x80
OSPF State Change	ospf.msg != 1
ICMP errors	icmp.type in { 3..5, 11 } icmpv6.type in { 1..4 }
ARP	arp
ICMP	icmp icmpv6
TCP RST	tcp.flags.reset eq 1
SCTP ABORT	sctp.chunk_type eq ABORT
TTL low or unexpected	(ip.dst != 224.0.0.4 && ip.ttl < 5 && !ipm && !ospf) (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl == 1 && !(vrrp carp))
Checksum Errors	eth.fcs.status=="Bad" ip.checksum.status=="Bad" tcp.checksum.status=="Bad" udp.checksum.status=="Bad" sctp.checksum.status=="Bad" mcastfcs.status=="Bad"
SMB	smb nbss nbns netbios
HTTP	http tcp.port == 80 http2
DCERPC	dcerpc
Routing	hsrp eigrp ospf bgp cdp vrrp carp gvrp igmp ismp
TCP SYN/FIN	tcp.flags & 0x02 tcp.flags.fin == 1
TCP	tcp
UDP	udp
Broadcast	eth[0] & 1
System Event	systemd_journal sysdig

Double click to edit. Drag to move. Rules are processed in order until a match is found.

+ - ⌂ ⌂ OK Copy from Cancel Import... Export... Help

5. Filtrado



File Edit View Go Capture **Analyze** Statistics Telephony Wireless Tools Help

Display Filters... Ctrl+Shift+F

Display Filter Macros... Ctrl+Shift+M

Display Filter Expression... Ctrl+Shift+E

No. Time Source Destination Info

24	0.258801661	34.192.168.1.100	192.168.1.101	HTTP/1.1 200 OK
25	1.803561027	10.192.168.1.100	192.168.1.101	[SYN]
26	1.829389123	10.192.168.1.100	192.168.1.101	[SYN]
27	1.960647335	194.150.169.131	10.0.2.15	[SYN]
28	1.9606692074	10.192.168.1.100	192.168.1.101	[SYN]
29	1.961213282	10.192.168.1.100	192.168.1.101	[SYN]
30	1.961831859	194.150.169.131	10.0.2.15	[SYN]
31	1.988412447	194.150.169.131	10.0.2.15	[SYN]
32	1.988472777	10.192.168.1.100	192.168.1.101	[SYN]
33	2.117237862	194.150.169.131	10.0.2.15	[SYN]
34	2.117311767	10.192.168.1.100	192.168.1.101	[SYN]
35	7.127740680	10.192.168.1.100	192.168.1.101	[SYN]
36	7.128863103	194.150.169.131	10.0.2.15	[SYN]
37	7.286069284	194.150.169.131	10.0.2.15	[SYN]
38	7.286089728	10.192.168.1.100	192.168.1.101	[SYN]
39	10.128892066	10.192.168.1.100	192.168.1.101	[SYN]
40	10.129461830	194.150.169.131	10.0.2.15	HTTP/1.1 200 OK
41	10.284979785	194.150.169.131	10.0.2.15	[ACK]
42	10.285005232	10.0.2.15	194.150.169.131	[ACK]

Protocol Length Info

TCP	60	443 → 38510 [ACK] Seq=1028 Ack=189 Seq=450
TCP	74	43408 → 80 [SYN] Seq=0 Win=642
TCP	74	43412 → 80 [SYN] Seq=0 Win=642
TCP	60	80 → 43408 [SYN, ACK] Seq=0 Ack=1
TCP	54	43408 → 80 [ACK] Seq=1 Ack=1 Win=642
HTTP	502	GET / HTTP/1.1
TCP	60	80 → 43408 [ACK] Seq=1 Ack=449
TCP	60	80 → 43412 [SYN, ACK] Seq=0 Ack=1
TCP	54	43412 → 80 [ACK] Seq=1 Ack=1 Win=642
HTTP	242	HTTP/1.1 304 Not Modified
TCP	54	43408 → 80 [ACK] Seq=449 Ack=1
TCP	54	43412 → 80 [FIN, ACK] Seq=1 Ack=1
TCP	60	80 → 43412 [ACK] Seq=1 Ack=2 Win=642
TCP	60	80 → 43412 [FIN, ACK] Seq=1 Ack=2
TCP	54	43412 → 80 [ACK] Seq=2 Ack=2
TCP	54	43408 → 80 [FIN, ACK] Seq=449 Ack=1
TCP	60	80 → 43408 [ACK] Seq=189 Ack=450
TCP	60	80 → 43408 [FIN, ACK] Seq=189 Ack=450
TCP	54	43408 → 80 [ACK] Seq=450 Ack=1

Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (672 bits) on interface eth0 at 00:00:27:cb:7e:f5 (PcsCompu_cb:7e:f5) [ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: 00:0c:29:00:00:00 (eth0)]
Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: 00:0c:29:00:00:00 (eth0)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.101
User Datagram Protocol, Src Port: 44487, Dst Port: 53
Domain Name System (query)

0000 52 54 00 12 35 02 08 00 27 cb 7e f5 08 00 45
00 4a ea 96 40 00 40 11 1f 54 0a 00 02 0f c0
0020 64 01 ad c7 00 35 00 36 31 00 35 7a 01 00 00
0030 00 00 00 00 00 00 07 63 6f 6e 74 69 6c 65 08
0040 65 72 76 69 63 65 73 07 6d 6f 7a 69 6c 6c 61
0050 63 6f 6d 00 00 01 00 01



Wireshark · Display Filters

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1	ip.addr != 192.0.2.1
IPv6 only	ipv6
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS port	!(udp.port == 53 tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80 udp.port == 80
HTTP	http
No ARP and no DNS	not arp and not dns
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and tcp.port not in {80, 25}

+ -

OK Cancel Help



Screenshot taken at 10:46 AM

Kali NetHunter • Exploit-DB • Google Hacking DB

[News] [Issues] [Tools] [Help]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

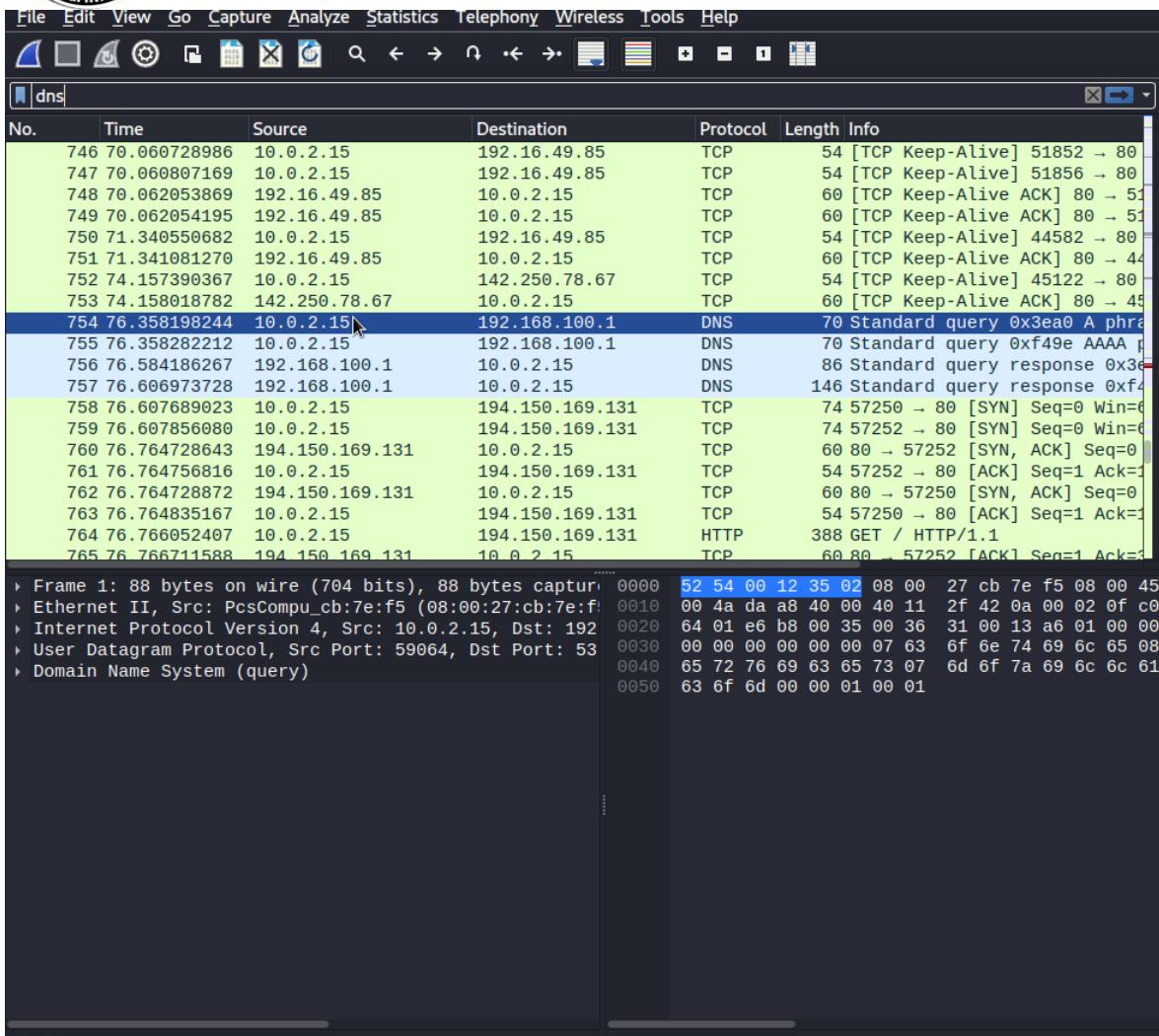
dns

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	10.0.2.15	10.0.2.3	DNS	88 Standard query 0xe5ff
2	0.000022332	10.0.2.15	10.0.2.3	DNS	88 Standard query 0xbef9
3	0.023482489	10.0.2.3	10.0.2.15	DNS	184 Standard query respons
5	0.030880075	10.0.2.3	10.0.2.15	DNS	169 Standard query respons
16	0.227172259	10.0.2.15	10.0.2.3	DNS	79 Standard query 0xfee9
17	0.227205498	10.0.2.15	10.0.2.3	DNS	79 Standard query 0xd9f9
18	0.269691514	10.0.2.3	10.0.2.15	DNS	148 Standard query respons
19	0.269752399	10.0.2.3	10.0.2.15	DNS	132 Standard query respons
43	0.667560480	10.0.2.15	10.0.2.3	DNS	70 Standard query 0x1be6
44	0.667591561	10.0.2.15	10.0.2.3	DNS	70 Standard query 0x07e4
50	0.696589491	10.0.2.3	10.0.2.15	DNS	133 Standard query respons
51	0.696740989	10.0.2.3	10.0.2.15	DNS	121 Standard query respons
69	1.067987266	10.0.2.15	10.0.2.3	DNS	70 Standard query 0x94b6
70	1.068015435	10.0.2.15	10.0.2.3	DNS	70 Standard query 0x04a8
75	1.123840123	10.0.2.3	10.0.2.15	DNS	86 Standard query respons
76	1.134116935	10.0.2.3	10.0.2.15	DNS	154 Standard query respons
91	1.469244986	10.0.2.15	10.0.2.3	DNS	76 Standard query 0xf0d4

Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (672 bits) on interface eth0 at 00:00:00:0c:29:3f [ether 00:00:00:0c:29:3f] at 10:46:10:46:01:01 len 88 (11:16 bytes, 11:16 bits)
Ethernet II, Src: PCSSystemec_d1:f8:5d (08:00:00:0c:29:3f), Dst: 08:00:00:00:00:00 (08:00:00:00:00:00) [ethertype IPv4 (0x0800), length 88]
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3 [ethertype IPv4 (0x0800), length 40]
User Datagram Protocol, Src Port: 49947, Dst Port: 53 [ethertype UDP (0x0806), length 36]
Domain Name System (query)

Packets: 1424 - Displayed: 138 (9.7%) - Dropped: 0 (0.0%) | Profile: Default

PsychoSpy





No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	192.168.100.1	DNS	88	Standard query 0x13a6 A cont
2	0.000377832	10.0.2.15	192.168.100.1	DNS	88	Standard query 0x6898 AAAA co
3	0.103972433	192.168.100.1	10.0.2.15	DNS	104	Standard query response 0x13
4	0.107447997	192.168.100.1	10.0.2.15	DNS	169	Standard query response 0x68
16	0.271726802	10.0.2.15	192.168.100.1	DNS	74	Standard query 0x245f A r3.c
17	0.271807840	10.0.2.15	192.168.100.1	DNS	74	Standard query 0x1859 AAAA r
18	0.319162422	192.168.100.1	10.0.2.15	DNS	173	Standard query response 0x24
19	0.382685495	192.168.100.1	10.0.2.15	DNS	197	Standard query response 0x18
27	0.486996754	10.0.2.15	192.168.100.1	DNS	95	Standard query 0x6765 A cont
28	0.488522382	10.0.2.15	192.168.100.1	DNS	95	Standard query 0x7a67 AAAA co
29	0.545795082	192.168.100.1	10.0.2.15	DNS	261	Standard query response 0x7a
30	0.557167040	192.168.100.1	10.0.2.15	DNS	249	Standard query response 0x67
86	1.487939733	10.0.2.15	192.168.100.1	DNS	85	Standard query 0x7fc2 A push
87	1.488118882	10.0.2.15	192.168.100.1	DNS	85	Standard query 0x9132 AAAA p
88	1.531281218	192.168.100.1	10.0.2.15	DNS	205	Standard query response 0x91
89	1.556021885	192.168.100.1	10.0.2.15	DNS	139	Standard query response 0x7f
90	1.601232134	10.0.2.15	192.168.100.1	DNS	85	Standard query 0xcf8d A push
91	1.601308621	10.0.2.15	192.168.100.1	DNS	85	Standard query 0xdc8f AAAA p
92	1.648659867	192.168.100.1	10.0.2.15	DNS	205	Standard query response 0xdd
93	1.666062975	192.168.100.1	10.0.2.15	DNS	139	Standard query response 0xd

Frame 1: 88 bytes on wire (704 bits), 88 bytes captured 0000 52 54 00 12 35 02 08 00 27 cb 7e f5 08 00 45
Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5) [0x0000], Dst: 192.168.100.1 (00:0c:29:00:00:01) [0x0000]
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.100.1 [0x0020]
User Datagram Protocol, Src Port: 59064, Dst Port: 53 [0x0030]
Domain Name System (query) [0x0040]

0050 63 6f 6d 00 00 01 00 01

Vamos a buscar un string

No.	Time	Source	Destination	Protocol	Length	Info

Find a packet

Packet list Narrow & Wide Case sensitive String pharck.org Find Cancel



```
618 29.207902543 192.168.100.1      10.0.2.15        DNS      219 Standard query response 0x23
+-- 754 76.358198244 10.0.2.15        192.168.100.1    DNS      70 Standard query 0x3ea0 A phr...
+-- 755 76.358282212 10.0.2.15        192.168.100.1    DNS      70 Standard query 0xf49e AAAA p...
+- 756 76.584186267 192.168.100.1    10.0.2.15        DNS      86 Standard query response 0x3e...
+- 757 76.606973728 192.168.100.1    10.0.2.15        DNS      146 Standard query response 0xf4

Frame 754: 70 bytes on wire (560 bits), 70 bytes captured
Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.100.1
User Datagram Protocol, Src Port: 54805, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x3ea0
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  -> Queries
    > phrack.org: type A, class IN
    [Response In: 756]
```

Todo petición debe tener una respuesta

```
754 76.358198244 10.0.2.15        192.168.100.1    DNS      70 Standard query 0x3ea0 A phr...
755 76.358282212 10.0.2.15        192.168.100.1    DNS      70 Standard query 0xf49e AAAA p...
756 76.584186267 192.168.100.1    10.0.2.15        DNS      86 Standard query response 0x3e...
757 76.606973728 192.168.100.1    10.0.2.15        DNS      146 Standard query response 0xf4

Frame 756: 86 bytes on wire (688 bits), 86 bytes captured
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: 192.168.100.1
Internet Protocol Version 4, Src: 192.168.100.1, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53, Dst Port: 54805
Domain Name System (response)
  Transaction ID: 0x3ea0
  Flags: 0x0180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  -> Queries
    > phrack.org: type A, class IN
  -> Answers
    > phrack.org: type A, class IN, addr 194.150.169.131
    [Request In: 754]
    [Time: 0.225988023 seconds]
```



..: Phrack Magazine :..

194.150.169.131

Kali Linux Kali Tools Kali Docs Kali Forums

[News] [Paper Feed] [Issues] [Authors] [Archives] [Contact]

.:: PHRACK NEWS ::.

Live and let die

posted by Phrack Staff

==Phrack Magazine==

C F P

P H R A C K 7 1

Dear readers, let's take a moment for poetry:



Capturar el trafico de una dirección ip

Ensamblar paquetes

Identificar un paquete y hacer el filtrado en este caso HTTP

The screenshot shows the Wireshark interface with a packet list. The 'Analyze' menu is open, and the 'Follow' submenu is selected. Within the 'Follow' submenu, 'HTTP Stream' is highlighted. The packet list shows several TCP and HTTP packets, with the last one selected.

Protocol	Length	Info
TCP	74	51290 → 80 [SYN]
TCP	60	80 → 51290 [SYN, ACK]
TCP	54	51290 → 80 [ACK]
HTTP	437	GET /index.html HTTP/1.1 200 OK
TCP	60	80 → 51290 [ACK]
TCP	1490	80 → 51290 [PSH, ACK]
TCP	54	51290 → 80 [ACK]
TCP	1514	80 → 51290 [ACK]
TCP	54	51290 → 80 [ACK]
TCP	5894	80 → 51290 [ACK]
TCP	54	51290 → 80 [ACK]



Wireshark · Follow HTTP Stream (tcp.stream eq 2) · eth0

```
Though much is taken, much abides; and tho'  
We are not now that strength which in old days  
Moved earth and heaven, that which we are,  
we are, [REDACTED]  
One equal temper of heroic hearts,  
Made weak by time and fate, but strong in will  
To strive, [REDACTED] to seek, to find,  
and not to yield [control].  
  
PHRACK 71 awaits your input, the impatient accepted will be sent strai  
ght to [REDACTED]  
our paperfeed.  
  
You know the rules:  
  
+ 7-bit ASCII  
+ English language  
+ DO USE OUR PGP KEY BELOW  
+ AND DO INCLUDE THE ANTISPAM KEYWORD  
  
Since the introduction of the paper feed feature, your submission has  
four [REDACTED]  
possible outcomes:  
  
1. The article is accepted, it can be published in the paper feed  
if [REDACTED]  
you want. Congratz.  
  
2. The article is accepted, but will be published in the final rel  
ease. [REDACTED]  
If you decide to contribute to PWN or linenoise (lul), this wil  
l be [REDACTED]  
the case. Nice one.  
  
3. The article is not *yet* suitable for PHRACK but nonetheless wo  
uld [REDACTED]  
be with additional work. A Phrack Staff reviewer is assigned to  
help [REDACTED]  
you to improve your paper. After improving it, it will be inclu  
  
Packet 32. 1 client pkt, 1 server pkt, 1 turn. Click to select.  
Entire conversation (10 kB) Show data as ASCII  
Find: Find Next  
Filter Out This Stream Print Save as... Back Close Help
```



Analizar paquetes de información

1. Ingresar a la siguiente pagina altoromutual.com



Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

[Sign In](#) | [Contact Us](#) | [Feedback](#) |

AltoroMutual

DEMO SITE ONLY

ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<p>PERSONAL</p> <ul style="list-style-type: none">Deposit ProductCheckingLoan ProductsCardsInvestments & InsuranceOther Services <p>SMALL BUSINESS</p> <ul style="list-style-type: none">Deposit ProductsLending ServicesCardsInsuranceRetirementOther Services <p>INSIDE ALTORO MUTUAL</p> <ul style="list-style-type: none">About UsContact UsLocationsInvestor RelationsPress RoomCareersSubscribe	<p>Online Banking with FREE Online Bill Pay</p> <p>No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.</p> <p>Real Estate Financing</p> <p>Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it.</p> <p>Business Credit Cards</p> <p>You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.</p> <p>Retirement Solutions</p> <p>Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.</p>	<p>Privacy and Security</p> <p>The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We provide you with the information and resources that you need to secure your information and keep it confidential. This is our priority.</p> <p>Win a Samsung Galaxy S10 smartphone</p> <p>Completing this short survey could put you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your input and feedback.</p>	

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from [GitHub](#) and take advantage of advanced features.

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting



[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search

AltoroMutual



ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
---	--------------------------	--------------------------------	--------------------------------------

PERSONAL

- [Deposit Product](#)
- [Checking](#)
- [Loan Products](#)
- [Cards](#)
- [Investments & Insurance](#)
- [Other Services](#)

SMALL BUSINESS

- [Deposit Products](#)
- [Lending Services](#)
- [Cards](#)
- [Insurance](#)
- [Retirement](#)
- [Other Services](#)

INSIDE ALTORO MUTUAL

- [About Us](#)
- [Contact Us](#)
- [Locations](#)
- [Investor Relations](#)
- [Press Room](#)
- [Careers](#)
- [Subscribe](#)

Online Banking Login



Username:

Password:

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc.

This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features.



← → ⌂ ⌂ altoromutual.com/login.jsp ⌂ ⌂ ⌂ ⌂ ⌂ ⌂

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search



ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
---	--------------------------	--------------------------------	--------------------------------------

PERSONAL

- [Deposit Product](#)
- [Checking](#)
- [Loan Products](#)
- [Cards](#)
- [Investments & Insurance](#)
- [Other Services](#)

SMALL BUSINESS

- [Deposit Products](#)
- [Lending Services](#)
- [Cards](#)
- [Insurance](#)
- [Retirement](#)
- [Other Services](#)

INSIDE ALTORO MUTUAL

- [About Us](#)
- [Contact Us](#)
- [Locations](#)
- [Investor Relations](#)
- [Press Room](#)
- [Careers](#)
- [Subscribe](#)

Online Banking Login

Login Failed: We're sorry, but this username or password was not found in our system. Please try again.

Username:

Password:

This connection is not secure.
Logins entered here could be compromised. [Learn More](#)

[View Saved Logins](#)

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc.

This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced fea

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SWI10>.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

2. Detener la captura y filtrar por HTTP



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
4	1.391780250	10.0.2.15	65.61.137.117	HTTP	500	GET /login.jsp HTTP/1.1
12	1.471680188	65.61.137.117	10.0.2.15	HTTP	68	HTTP/1.1 200 OK (text/ht
24	25.757629577	10.0.2.15	65.61.137.117	HTTP	644	POST /doLogin HTTP/1.1 (
26	25.837559656	65.61.137.117	10.0.2.15	HTTP	180	HTTP/1.1 302 Found
28	25.866233636	10.0.2.15	65.61.137.117	HTTP	500	GET /login.jsp HTTP/1.1
32	25.946552219	65.61.137.117	10.0.2.15	HTTP	4471	HTTP/1.1 200 OK (text/ht



http

No.	Time	Source	Destination	Protocol	Length	Info
4	1.391780250	10.0.2.15	65.61.137.117	HTTP	500	GET /login.jsp HTTP/1.1
12	1.471680188	Mark/Unmark Packet	Ctrl+M	HTTP	68	HTTP/1.1 200 OK (text/html)
24	25.757629577	Ignore/Unignore Packet	Ctrl+D	HTTP	644	POST /doLogin HTTP/1.1 (
26	25.837559656	Set/Unset Time Reference	Ctrl+T	HTTP	180	HTTP/1.1 302 Found
28	25.866233636	Time Shift...	Ctrl+Shift+T	HTTP	500	GET /login.jsp HTTP/1.1
32	25.946552219	Packet Comments	>	HTTP	4471	HTTP/1.1 200 OK (text/html)
		Edit Resolved Name				
		Apply as Filter	>			
		Prepare as Filter	>			
		Conversation Filter	>			
		Colorize Conversation	>			
		SCTP	>			
		Follow	>	TCP Stream	Ctrl+Alt+Shift+T	
		Copy	>	UDP Stream	Ctrl+Alt+Shift+U	b 7e f5 08 0
		Protocol Preferences	>	DCCP Stream	Ctrl+Alt+Shift+E	2 0a 00 02 0
		Decode As...		TLS Stream	Ctrl+Alt+Shift+S	5 1e 41 1e 0
		Show Packet in New Window		HTTP Stream	Ctrl+Alt+Shift+H	0 2f 6c 6f 6
						f 31 2e 31 0
						2 6f 6d 75 7
						5 72 2d 41 6
						1 2f 35 2e 3
						8 20 78 38 3
						e 30 29 20 4
						2 6f 6d 75 7
						5 72 2d 41 6
						1 2f 35 2e 3
						8 20 78 38 3
						e 30 29 20 4
00a0		6b 6f 2f 32 30 31 30 30 31 30 31 20 46 6				
00b0		66 6f 78 2f 31 31 35 2e 30 0d 0a 41 63 6				
00c0		74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 6				
00d0		6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6				
00e0		6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6				
00f0		6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 6				
0100		76 69 66 2c 69 6d 61 67 65 2f 77 65 62 7				
0110		2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 6				
0120		2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2				
0130		2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 6				
0140		74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7				
0150		2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6				



Wireshark · Follow HTTP Stream (tcp.stream eq 1) · eth0

```
POST /doLogin HTTP/1.1
Host: altoromutual.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Origin: http://altoromutual.com
Connection: keep-alive
Referer: http://altoromutual.com/login.jsp
Cookie: JSESSIONID=DE333B98ADF5D133D0871F281B14F591
Upgrade-Insecure-Requests: 1

uid=fabian+&passw=ememejejd&btnSubmit=LoginHTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Thu, 14 Sep 2023 14:29:09 GMT

GET /login.jsp HTTP/1.1
Host: altoromutual.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://altoromutual.com/login.jsp
Connection: keep-alive
Cookie: JSESSIONID=DE333B98ADF5D133D0871F281B14F591
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 14 Sep 2023 14:29:09 GMT

2 client pkts, 2 server pkts, 3 turns.

Entire conversation (9,939 bytes) Show data as ASCII
Find: Find Next
```



TCP DUMP

(herramienta de consola la cual usa comandos)

1. abrir consola y entrar como root y dar el siguiente comando tcpdump -h

```
[root@kali]# ./tcpdump -h
tcpdump version 4.99.4
libpcap version 1.10.4 (with TPACKET_V3)
OpenSSL 3.0.10 1 Aug 2023
Usage: tcpdump [-AbdDefnHIJKLMNOPqStuUvxX#] [ -B size ] [ -c count ] [--count]
[ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
[ -i interface ] [ --immediate-mode ] [ -j tstamptype ]
[ -M secret ] [ --number ] [ --print ] [ -Q in|out|inout ]
[ -r file ] [ -s snaplen ] [ -T type ] [ --version ]
[ -V file ] [ -w file ] [ -W filecount ] [ -y datalinktype ]
[ --time-stamp-precision precision ] [ --micro ] [ --nano ]
[ -z postrotate-command ] [ -Z user ] [ expression ]
```

2. tcpdump -D

```
[root@kali]# ./tcpdump -D
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7 dbus-system (D-Bus system bus) [none]
8 dbus-session (D-Bus session bus) [none]
```

3. tcpdump -i eth0

```
[root@kali]# ./tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```



```
File Actions Edit View Help
root@kali: /home/kali
File Actions Edit View Help
10:42:12.474139 IP 10.0.2.15.41516 > 194.150.169.131.http: Flags [P.], seq 1:335, ack 1, win 64240, length 334: HTTP: GET / HTTP/1.1
10:42:12.475055 IP 194.150.169.131.http > 10.0.2.15.41516: Flags [.], ack 335, win 65535, length 0
10:42:12.475480 IP 10.0.2.15.41516 > 194.150.169.131.http: Flags [F.], seq 335, ack 1, win 64240, length 0
10:42:12.476228 IP 194.150.169.131.http > 10.0.2.15.41516: Flags [.], ack 336, win 65535, length 0
10:42:12.631447 IP 194.150.169.131.http > 10.0.2.15.41516: Flags [.], seq 1:2921, ack 336, win 65535, length 2920: HTTP: HTTP/1.1 200 OK
10:42:12.631657 IP 10.0.2.15.41516 > 194.150.169.131.http: Flags [R], seq 915458585, win 0, length 0
10:42:12.671999 IP 10.0.2.15.41518 > 194.150.169.131.http: Flags [S], seq 1536381114, win 64240, options [mss 1460,sackOK,TS val 4143220263 ecr 0,nop,wscale 7], length 0
10:42:12.677992 IP 10.0.2.15.41530 > 194.150.169.131.http: Flags [S], seq 1312838445, win 64240, options [mss 1460,sackOK,TS val 4143220269 ecr 0,nop,wscale 7], length 0
10:42:12.697260 IP 10.0.2.15.41546 > 194.150.169.131.http: Flags [S], seq 1363159058, win 64240, options [mss 1460,sackOK,TS val 4143220288 ecr 0,nop,wscale 7], length 0
10:42:12.824988 IP 192.168.100.1.domain > 10.0.2.15.39716: 7803 NXDomain 0/1/0 (113)
10:42:12.826265 IP 194.150.169.131.http > 10.0.2.15.41518: Flags [S.], seq 610432001, ack 1536381115, win 65535, options [mss 1460], length 0
10:42:12.826279 IP 10.0.2.15.41518 > 194.150.169.131.http: Flags [R], seq 1536381115, win 0, length 0
10:42:12.837954 IP 194.150.169.131.http > 10.0.2.15.41530: Flags [S.], seq 610496001, ack 1312838446, win 65535, options [mss 1460], length 0
10:42:12.837975 IP 10.0.2.15.41530 > 194.150.169.131.http: Flags [R], seq 1312838446, win 0, length 0
10:42:12.854661 IP 194.150.169.131.http > 10.0.2.15.41546: Flags [S.], seq 610560001, ack 1363159059, win 65535, options [mss 1460], length 0
10:42:12.854695 IP 10.0.2.15.41546 > 194.150.169.131.http: Flags [R], seq 1363159059, win 0, length 0
10:42:13.893877 IP 10.0.2.15.41548 > 194.150.169.131.http: Flags [S], seq 2674591055, win 64240, options [mss 1460,sackOK,TS val 4143221484 ecr 0,nop,wscale 7], length 0
10:42:14.049010 IP 194.150.169.131.http > 10.0.2.15.41548: Flags [S.], seq 610816001, ack 2674591056, win 65535, options [mss 1460], length 0
10:42:14.049036 IP 10.0.2.15.41548 > 194.150.169.131.http: Flags [.], ack 1, win 64240, length 0
10:42:19.050895 IP 10.0.2.15.41548 > 194.150.169.131.http: Flags [F.], seq 1, ack 1, win 64240, length 0
10:42:19.051321 IP 194.150.169.131.http > 10.0.2.15.41548: Flags [.], ack 2, win 65535, length 0
10:42:19.205455 IP 194.150.169.131.http > 10.0.2.15.41548: Flags [F.], seq 1, ack 2, win 65535, length 0
10:42:19.205472 IP 10.0.2.15.41548 > 194.150.169.131.http: Flags [.], ack 2, win 64240, length 0
```

```
tcpdump -v -i eth0
```



```
[root@kali]~[/home/kali]
# tcpdump -v -i eth0
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:45:24.700739 IP (tos 0x0, ttl 64, id 29032, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.55960 > bog02s16-in-f3.1e100.net.http: Flags [.], cksum 0xe966 (incorrect → 0xfb6e),
ack 633984703, win 63791, length 0
10:45:24.701391 IP (tos 0x0, ttl 64, id 8373, offset 0, flags [none], proto TCP (6), length 40)
    bog02s16-in-f3.1e100.net.http > 10.0.2.15.55960: Flags [.], cksum 0xf49d (correct), ack 1, win 6
5535, length 0
10:45:24.765091 IP (tos 0x0, ttl 64, id 35330, offset 0, flags [DF], proto UDP (17), length 72)
    10.0.2.15.56156 > 192.168.100.1.domain: 42293+ PTR? 67.78.250.142.in-addr.arpa. (44)
10:45:24.804919 IP (tos 0x0, ttl 64, id 8374, offset 0, flags [none], proto UDP (17), length 110)
    192.168.100.1.domain > 10.0.2.15.56156: 42293 1/0/0 67.78.250.142.in-addr.arpa. PTR bog02s16-in-
f3.1e100.net. (82)
10:45:24.805431 IP (tos 0x0, ttl 64, id 2461, offset 0, flags [DF], proto UDP (17), length 68)
    10.0.2.15.41906 > 192.168.100.1.domain: 58392+ PTR? 15.2.0.10.in-addr.arpa. (40)
10:45:24.834626 IP (tos 0x0, ttl 64, id 8375, offset 0, flags [none], proto UDP (17), length 68)
    192.168.100.1.domain > 10.0.2.15.41906: 58392 NXDomain 0/0/0 (40)
```

tcpdump icmp

```
[root@kali]~[/home/kali]
# tcpdump icmp
tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```



The terminal window displays two sessions. The left session shows the output of a 'tcpdump' command capturing ICMP traffic on interface 'eth0'. The right session shows the output of a 'ping google.com' command.

```
File Actions Edit View Help
File Actions Edit View Help
root@kali: /home/kali
root@kali: ~
File Actions Edit View Help
File Actions Edit View Help
(kali㉿kali)-[~]
$ ping google.com
PING google.com (142.250.78.78) 56(84) bytes of data.
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=1 ttl=113
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=2 ttl=113
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=3 ttl=113
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=4 ttl=113
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=5 ttl=113
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=6 ttl=113
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=7 ttl=113
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=8 ttl=113
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=9 ttl=113
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=10 ttl=113
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=11 ttl=113
^C
— google.com ping statistics —
11 packets transmitted, 11 received, 0% packet loss, time 10023ms
rtt min/avg/max/mdev = 5.173/6.007/9.391/1.160 ms
(kali㉿kali)-[~]
$
```

```
tcpdump -i eth0 -w Desktop/captura.pcap
```

The terminal window shows the command 'tcpdump -i eth0 -w Desktop/captura.pcap' being entered.

```
(root㉿kali)-[~/kali]
# tcpdump -i eth0 -w Desktop/captura.pcap
```

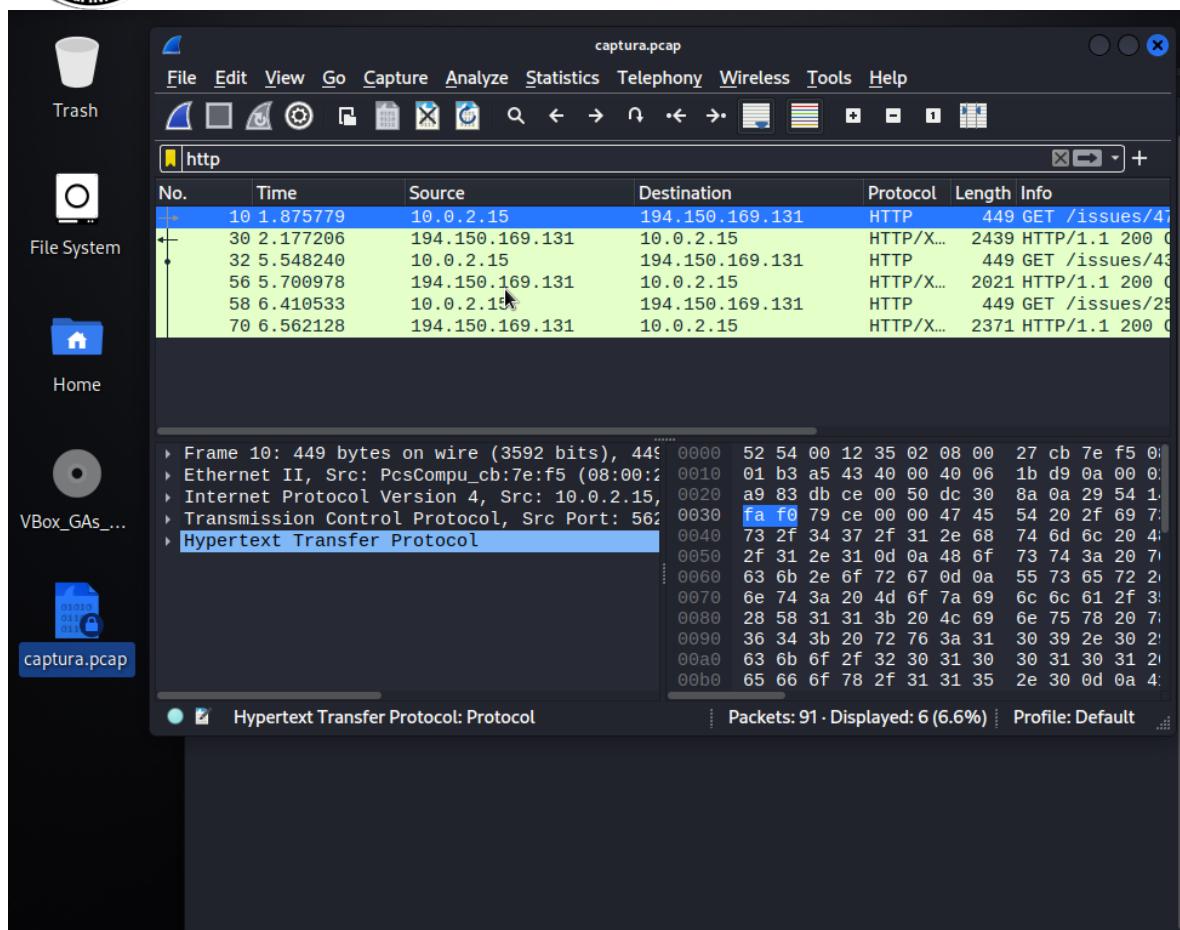


The screenshot shows a terminal window titled "root@kali: /home/kali". The terminal displays the following command and its output:

```
(root㉿kali)-[~/home/kali]
# tcpdump -i eth0 -w Desktop/captura.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C91 packets captured
91 packets received by filter
0 packets dropped by kernel

(root㉿kali)-[~/home/kali]
#
```

The terminal window is part of a desktop environment, with a sidebar on the left containing icons for Trash, File System, Home, and a file named "captura.pcap". The desktop background features a watermark of the Kali logo.



Tcpdump -r captura.pcap



```
[root@kali]~# tcpdump -r captura.pcap
```

```
[root@kali]~# tcpdump -r captura.pcap
reading from file captura.pcap, link-type EN10MB (Ethernet), snapshot length 262144
10:53:04.209365 IP 10.0.2.15.48778 > 192.168.100.1.domain: 47427+ A? phrack.org. (28)
10:53:04.298409 IP 192.168.100.1.domain > 10.0.2.15.48778: 47427 1/0/0 A 194.150.169.131 (44)
10:53:04.298700 IP 10.0.2.15.56270 > 194.150.169.131.http: Flags [S], seq 3694168585, win 64240, options [mss 1460,sackOK,TS val 4143871889 ecr 0,nop,wscale 7], length 0
10:53:04.448812 IP 194.150.169.131.http > 10.0.2.15.56270: Flags [S.], seq 693376001, ack 3694168586, win 65535, options [mss 1460], length 0
10:53:04.448842 IP 10.0.2.15.56270 > 194.150.169.131.http: Flags [.], ack 1, win 64240, length 0
10:53:04.875397 IP 55.65.117.34.bc.googleusercontent.com.https > 10.0.2.15.46246: Flags [P.], seq 655233155:655233179, ack 1224361907, win 65535, length 24
10:53:04.875419 IP 10.0.2.15.46246 > 55.65.117.34.bc.googleusercontent.com.https: Flags [.], ack 24, win 64022, length 0
10:53:04.876003 IP 10.0.2.15.46246 > 55.65.117.34.bc.googleusercontent.com.https: Flags [P.], seq 1:29, ack 24, win 64022, length 28
10:53:04.876842 IP 55.65.117.34.bc.googleusercontent.com.https > 10.0.2.15.46246: Flags [.], ack 29, win 65535, length 0
10:53:06.085144 IP 10.0.2.15.56270 > 194.150.169.131.http: Flags [P.], seq 1:396, ack 1, win 64240, length 395: HTTP: GET /issues/47/1.html HTTP/1.1
10:53:06.085564 IP 194.150.169.131.http > 10.0.2.15.56270: Flags [.], ack 396, win 65535, length 0
10:53:06.236019 IP 194.150.169.131.http > 10.0.2.15.56270: Flags [P.], seq 1:1437, ack 396, win 65535, length 1436: HTTP: HTTP/1.1 200 OK
10:53:06.236054 IP 10.0.2.15.56270 > 194.150.169.131.http: Flags [.], ack 1437, win 63184, length 0
10:53:06.237802 IP 194.150.169.131.http > 10.0.2.15.56270: Flags [.], seq 1437:5817, ack 396, win 65535, length 4380: HTTP
10:53:06.237815 IP 10.0.2.15.56270 > 194.150.169.131.http: Flags [.], ack 5817, win 61320, length 0
10:53:06.238738 IP 194.150.169.131.http > 10.0.2.15.56270: Flags [.], seq 5817:11657, ack 396, win 6
```

tcpdump -n port 53 -v -r captura.pcap

```
[root@kali]~# tcpdump -n port 53 -v -r captura.pcap
reading from file captura.pcap, link-type EN10MB (Ethernet), snapshot length 262144
10:53:04.209365 IP (tos 0x0, ttl 64, id 52686, offset 0, flags [DF], proto UDP (17), length 56)
    10.0.2.15.48778 > 192.168.100.1.53: 47427+ A? phrack.org. (28)
10:53:04.298409 IP (tos 0x0, ttl 64, id 8544, offset 0, flags [none], proto UDP (17), length 72)
    192.168.100.1.53 > 10.0.2.15.48778: 47427 1/0/0 phrack.org. A 194.150.169.131 (44)
10:53:19.528543 IP (tos 0x0, ttl 64, id 39102, offset 0, flags [DF], proto UDP (17), length 62)
    10.0.2.15.51175 > 192.168.100.1.53: 3465+ A? altoromutual.com. (34)
10:53:19.726736 IP (tos 0x0, ttl 64, id 8600, offset 0, flags [none], proto UDP (17), length 78)
    192.168.100.1.53 > 10.0.2.15.51175: 3465 1/0/0 altoromutual.com. A 65.61.137.117 (50)
```