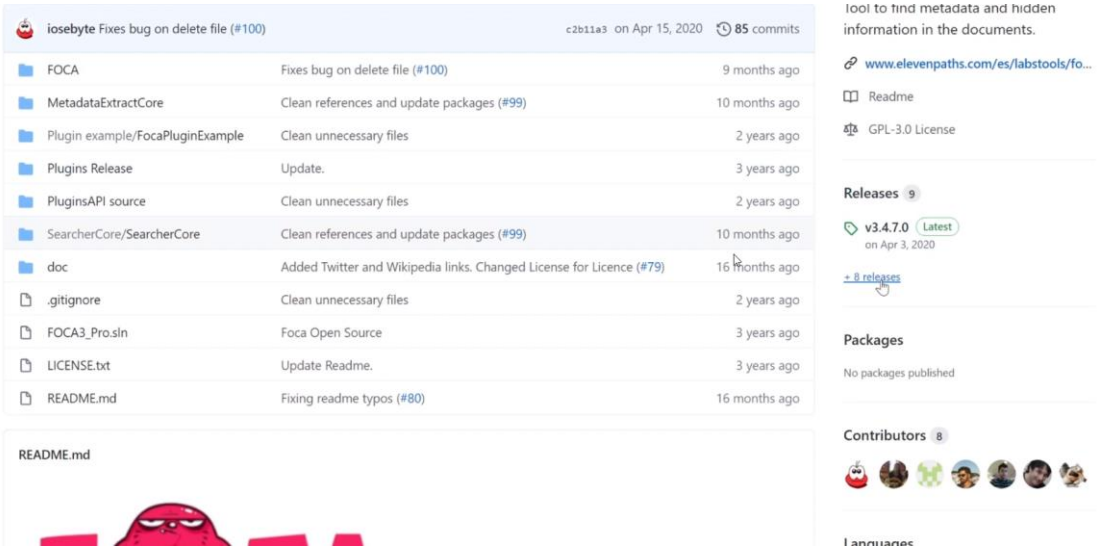
RECOLECCION SEMI PASIVA DE INFORMACION

FOCA

1. Virtualizar el SO de un Windows 10

2. Ya virtualizado descargar FOCA

3. Ir a releases y descargar la ultima versión



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.

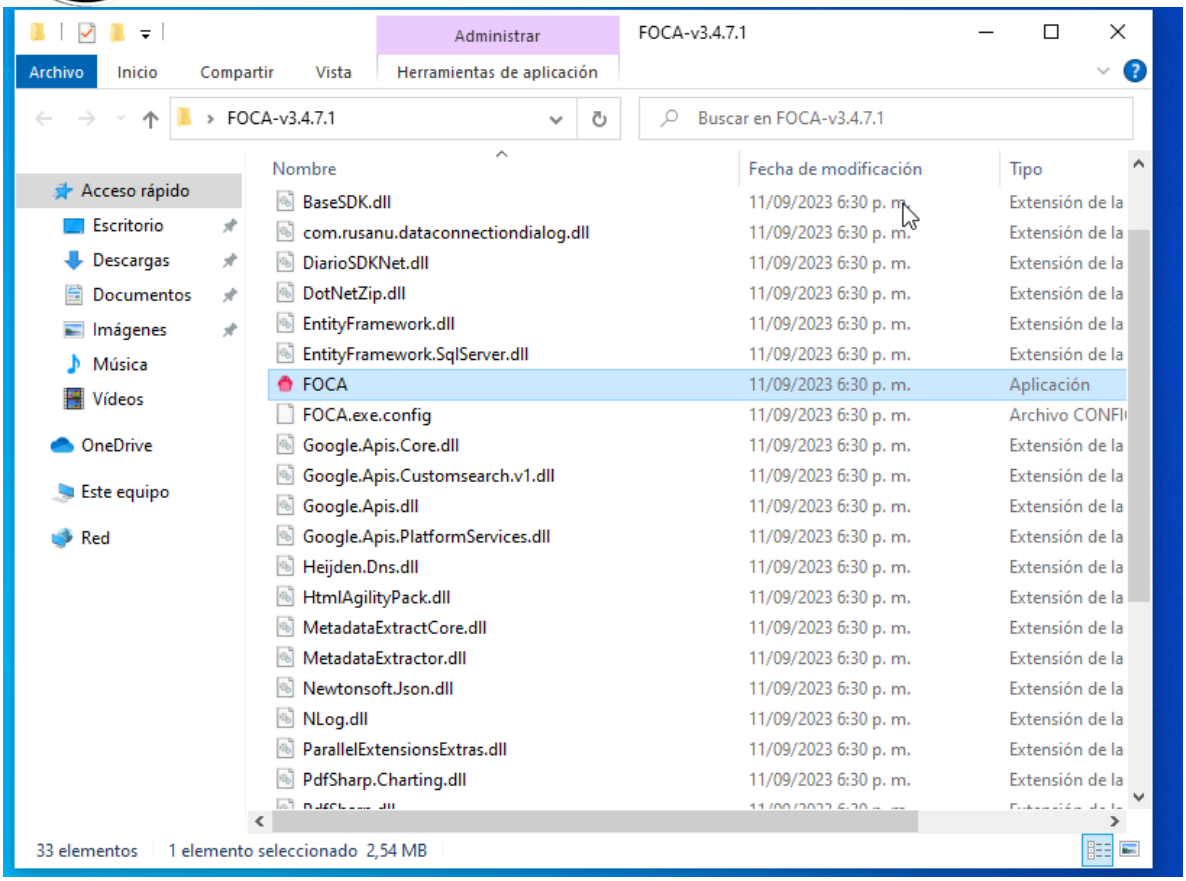
Download now

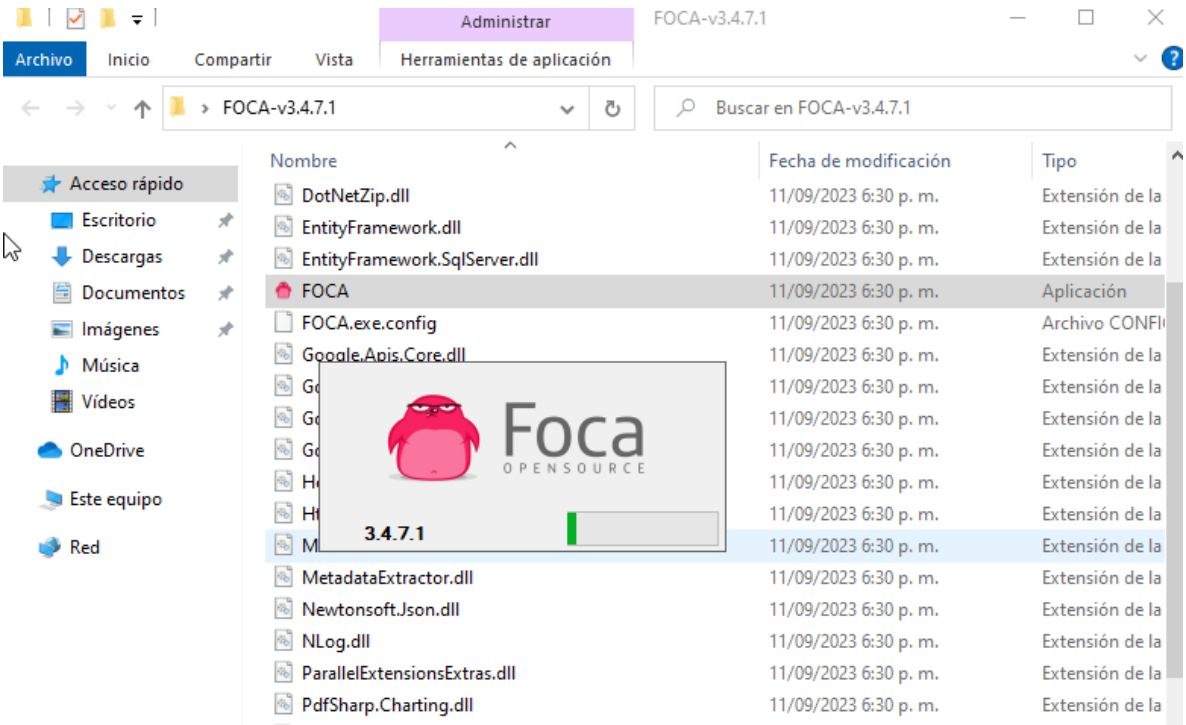
Express

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

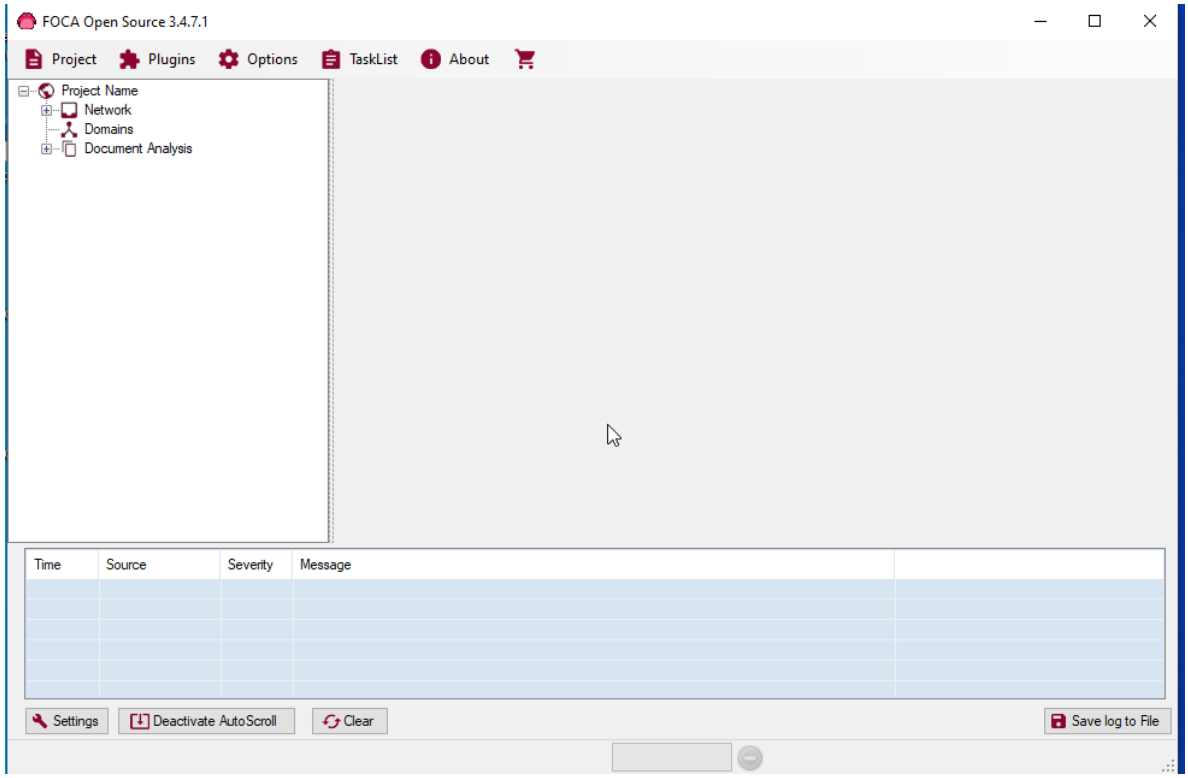
Download now

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

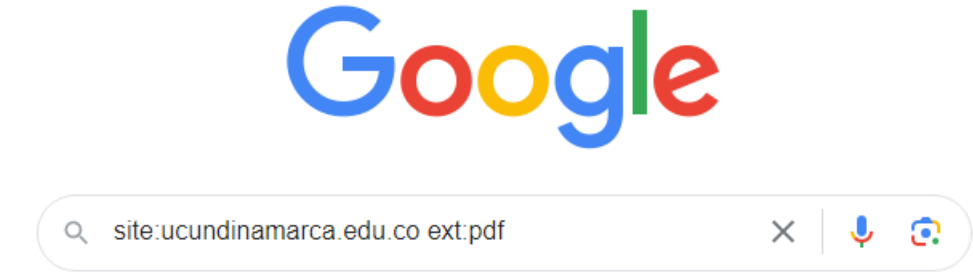

Administrar
FOCA-v3.4.7.1
Archivo
Inicio
Compartir
Vista
Herramientas de aplicación
FOCA-v3.4.7.1
Buscar en FOCA-v3.4.7.1
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
Música
Vídeos
OneDrive
Este equipo
Red
Nombre
Fecha de modificación
Tipo
BaseSDK.dll 11/09/2023 6:30 p. m. Extensión de la
com.rusanu.dataconnectiondialog.dll 11/09/2023 6:30 p. m. Extensión de la
DiarioSDKNet.dll 11/09/2023 6:30 p. m. Extensión de la
DotNetZip.dll 11/09/2023 6:30 p. m. Extensión de la
EntityFramework.dll 11/09/2023 6:30 p. m. Extensión de la
EntityFramework.SqlServer.dll 11/09/2023 6:30 p. m. Extensión de la
FOCA 11/09/2023 6:30 p. m. Aplicación
FOCA.exe.config 11/09/2023 6:30 p. m. Archivo CONFI
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
33 elementos
1 elemento seleccionado 2,54 MB

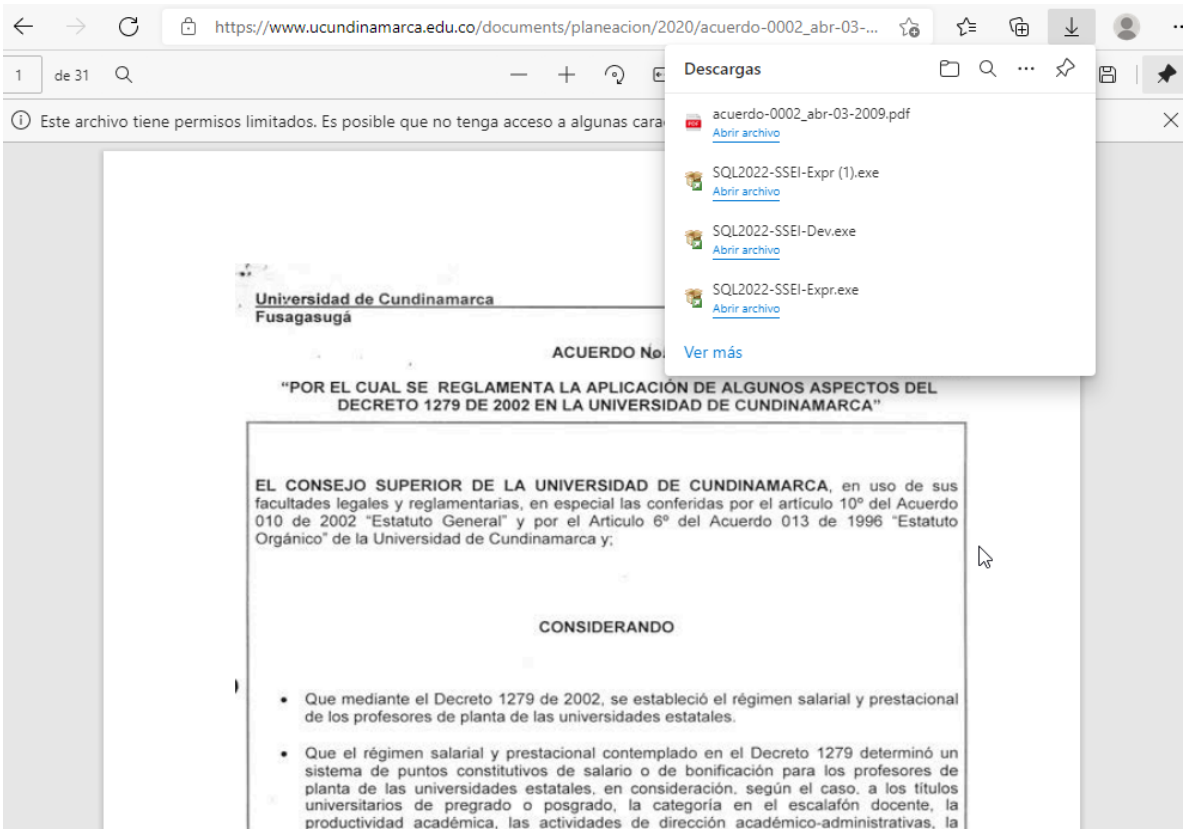

Administrar
FOCA-v3.4.7.1
Archivo
Inicio
Compartir
Vista
Herramientas de aplicación
FOCA-v3.4.7.1
Buscar en FOCA-v3.4.7.1
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
Música
Vídeos
OneDrive
Este equipo
Red
Nombre
Fecha de modificación
Tipo
DotNetZip.dll 11/09/2023 6:30 p. m. Extensión de la
EntityFramework.dll 11/09/2023 6:30 p. m. Extensión de la
EntityFramework.SqlServer.dll 11/09/2023 6:30 p. m. Extensión de la
FOCA 11/09/2023 6:30 p. m. Aplicación
FOCA.exe.config 11/09/2023 6:30 p. m. Archivo CONFI
Google.Apis.Core.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
Foca
OPENSOURCE
3.4.7.1

6. Bienvenido a FOCA

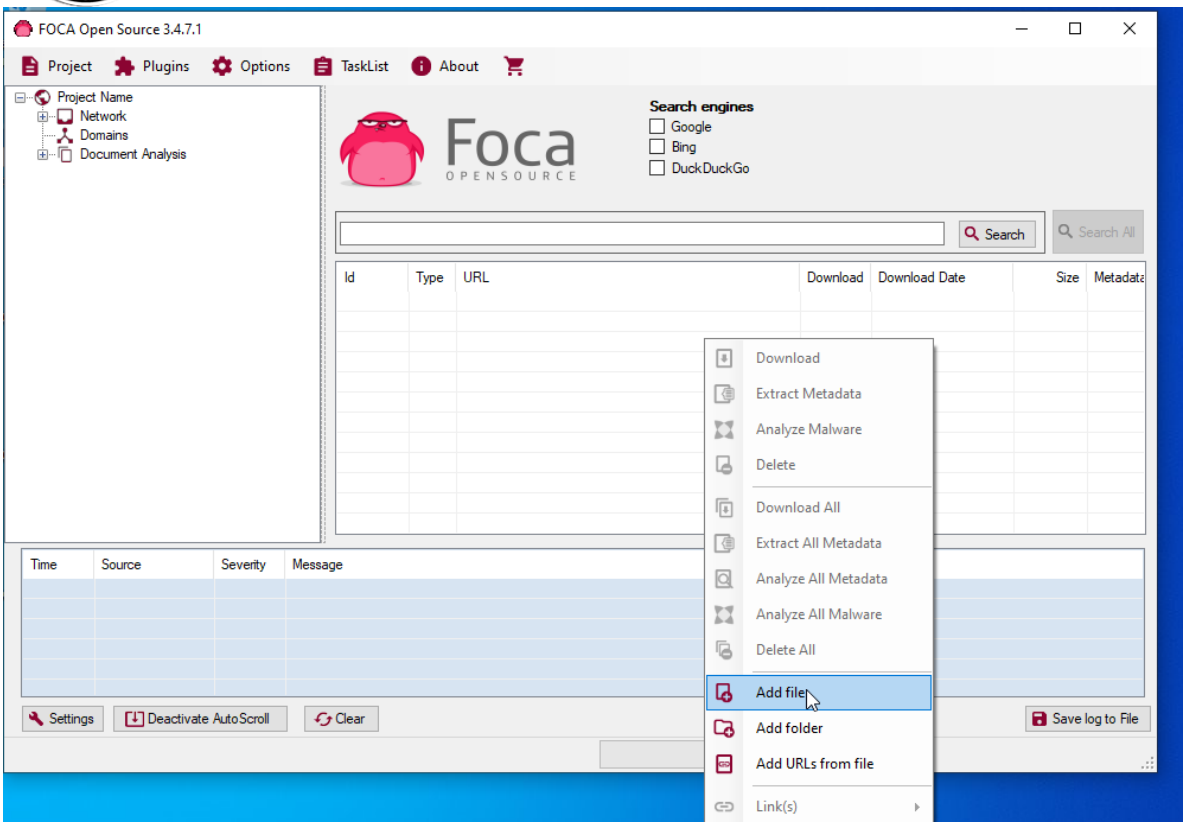


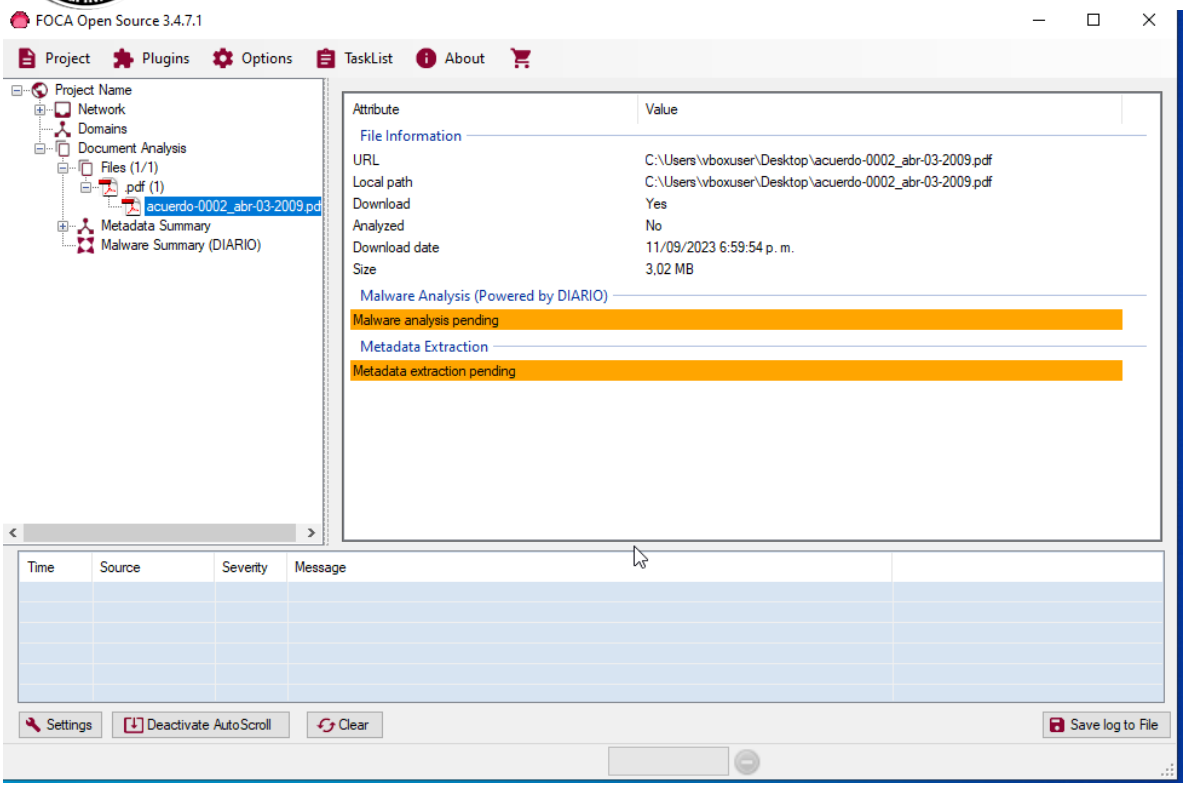
7. Descargar un fichero en Google para empezar a hacer una prueba sencilla de el uso de FOCA.



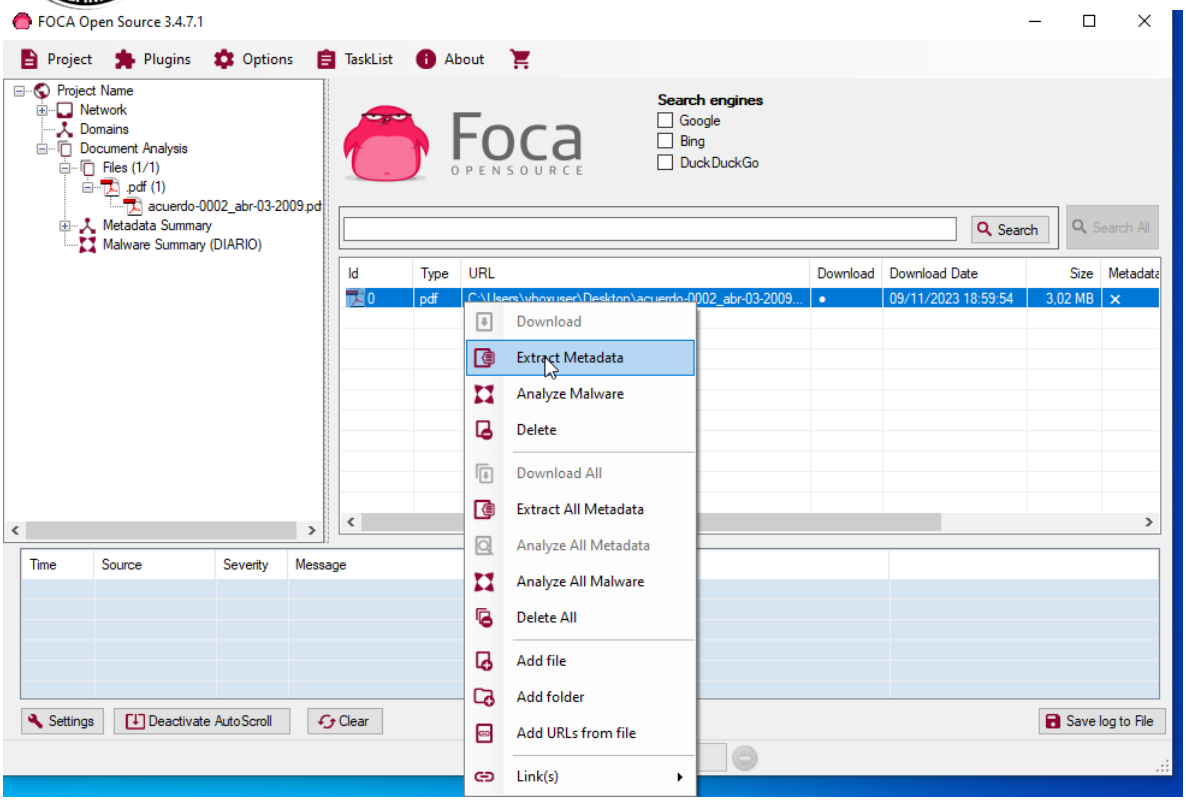


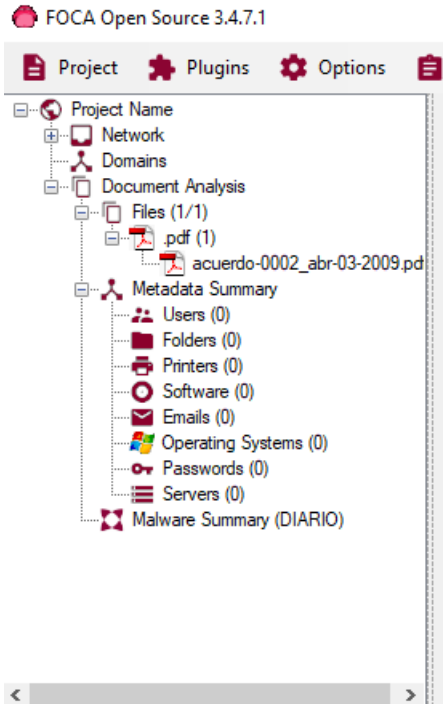
8. Ir a Document Analysis y en el grafo dar clic derecho y add file

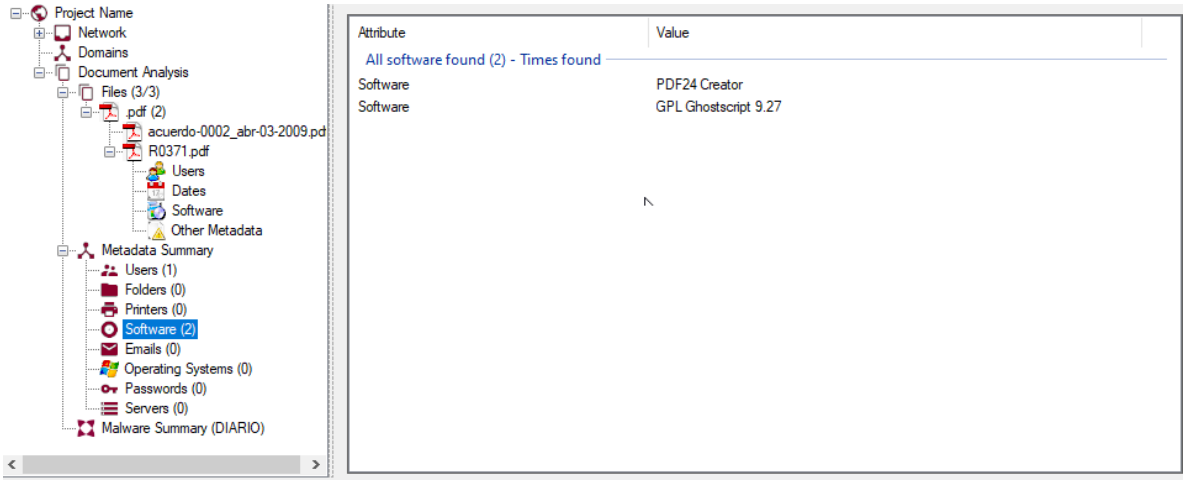

FOCA Open Source 3.4.7.1
Project
Plugins
Options
TaskList
About
Project Name
Network
Domains
Document Analysis
Foca
OPENSOURCE
Search engines
Google
Bing
DuckDuckGo
Search
Search All
Id
Type
URL
Download
Download Date
Size
Metadata
Download
Extract Metadata
Analyze Malware
Delete
Download All
Extract All Metadata
Analyze All Metadata
Analyze All Malware
Delete All
Add file
Add folder
Add URLs from file
Link(s)
Time
Source
Severity
Message
Settings
Deactivate AutoScroll
Clear
Save log to File



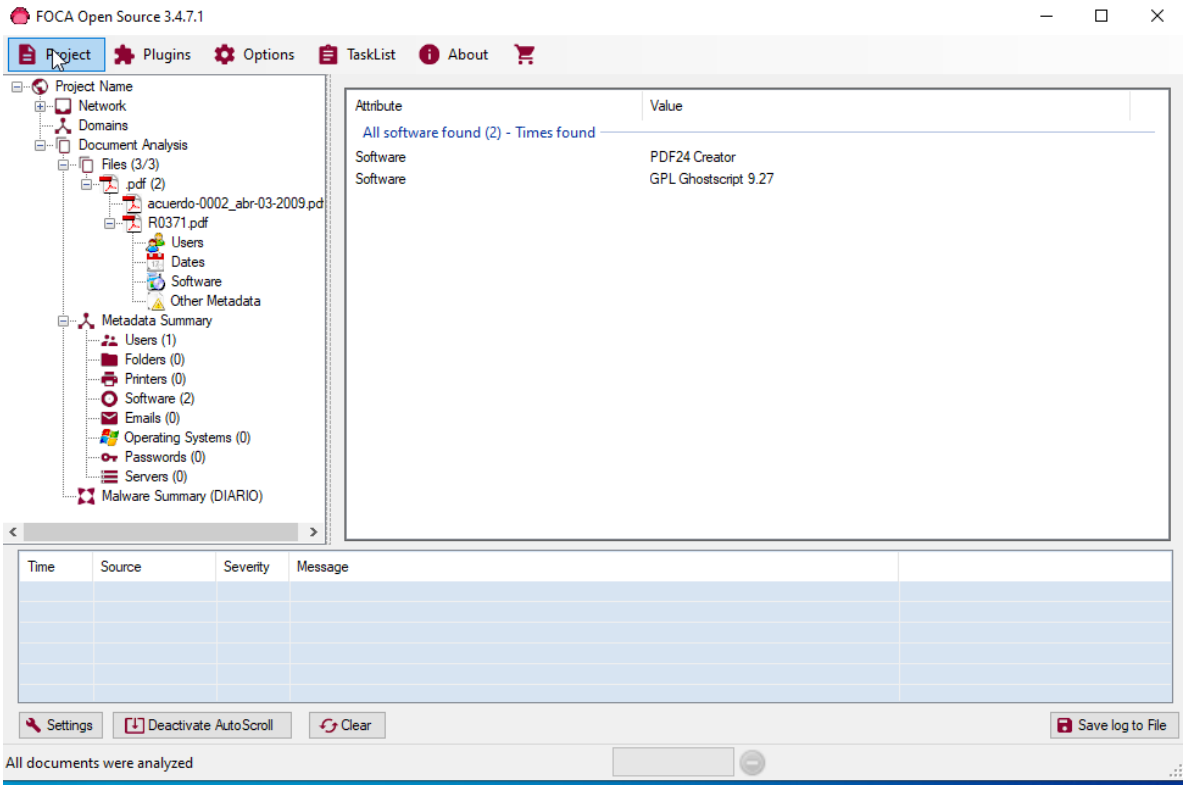
9. Como se evidencia no se ha realizado el análisis de metadata volvemos a document y extraemos la metadata

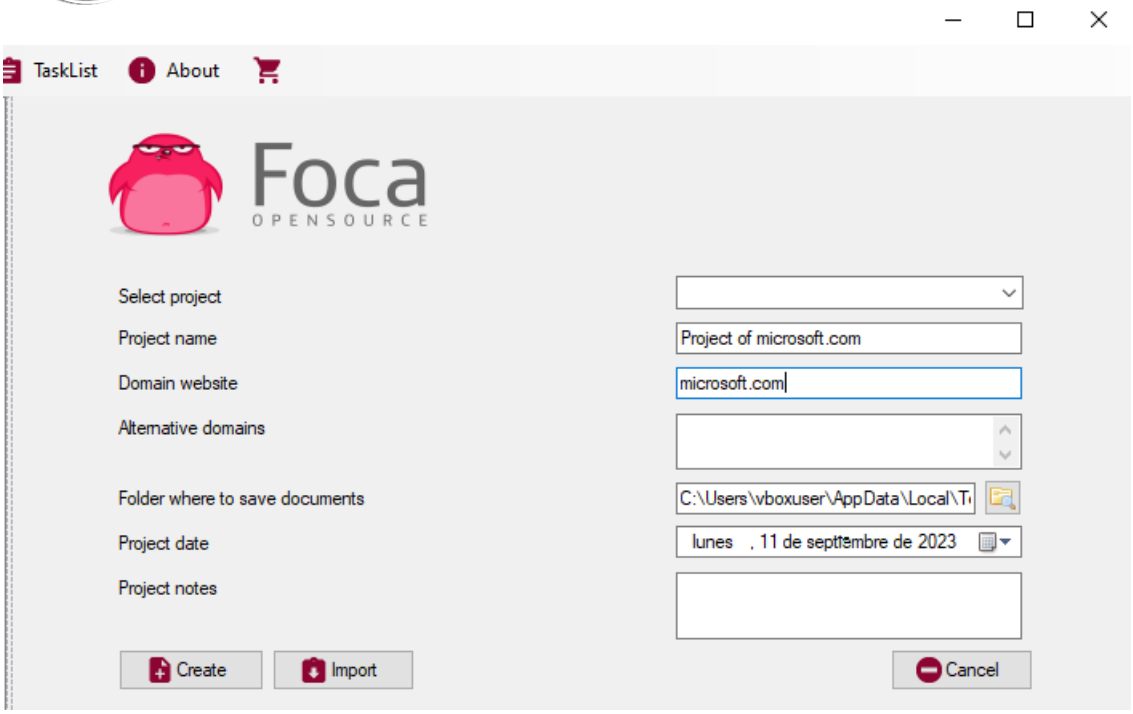

FOCA Open Source 3.4.7.1
Project
Plugins
Options
TaskList
About
Project Name
Network
Domains
Document Analysis
Files (1/1)
.pdf (1)
acuerdo-0002_abr-03-2009.pd
Metadata Summary
Malware Summary (DIARIO)
Foca
OPENSOURCE
Search engines
Google
Bing
DuckDuckGo
Search
Search All
Id
Type
URL
Download
Download Date
Size
0
pdf
09/11/2023 18:59:54
3,02 MB
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)
Time
Source
Severity
Message
Settings
Deactivate AutoScroll
Clear
Save log to File

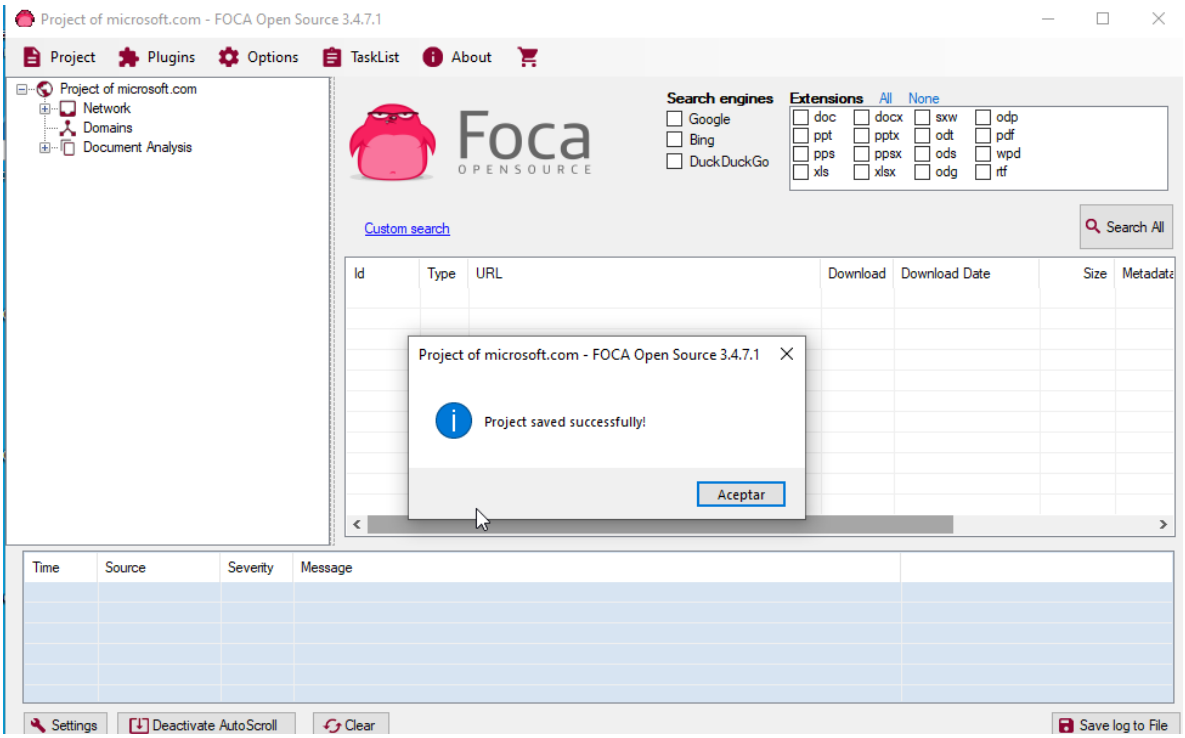

FOCA Open Source 3.4.7.1
Project
Plugins
Options
Project Name
Network
Domains
Document Analysis
Files (1/1)
.pdf (1)
acuerdo-0002_abr-03-2009.pd
Metadata Summary
Users (0)
Folders (0)
Printers (0)
Software (0)
Emails (0)
Operating Systems (0)
Passwords (0)
Servers (0)
Malware Summary (DIARIO)

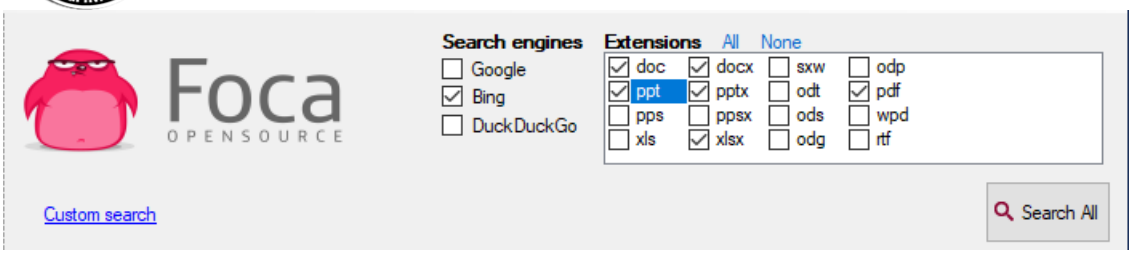


10. Crearemos un proyecto para evitar la búsqueda uno a uno

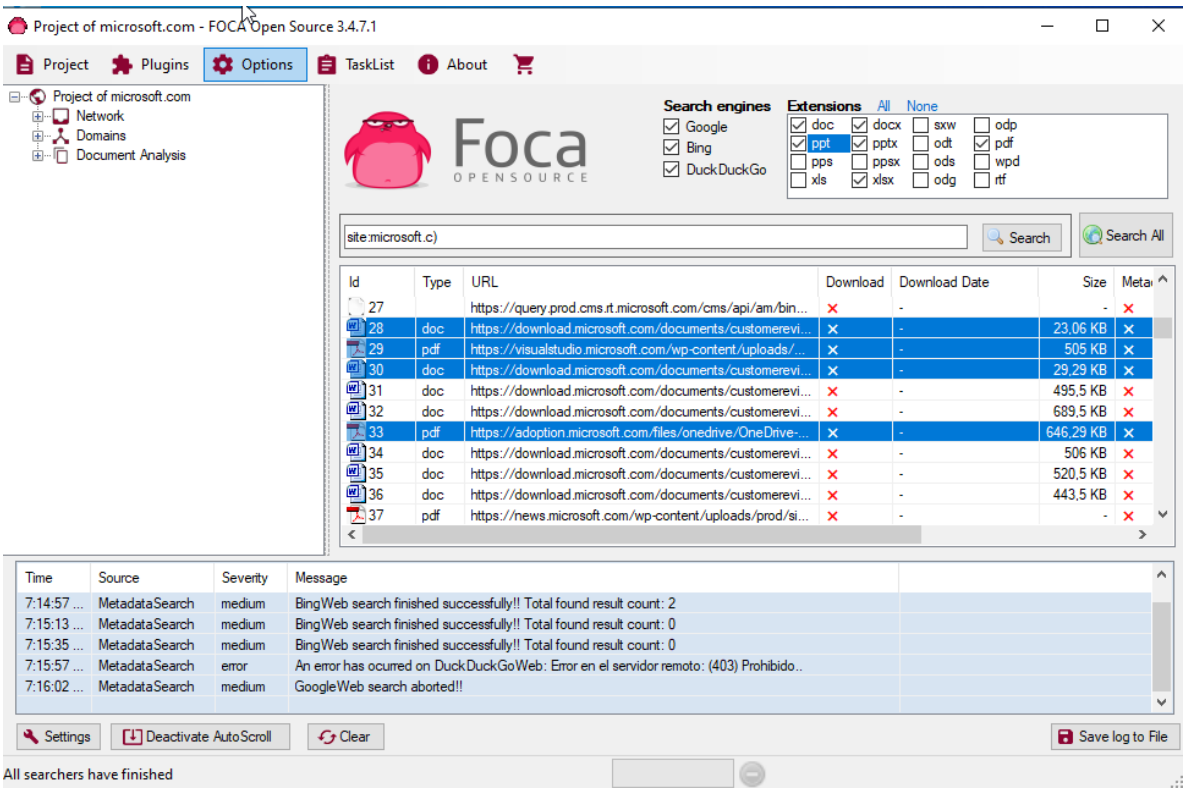


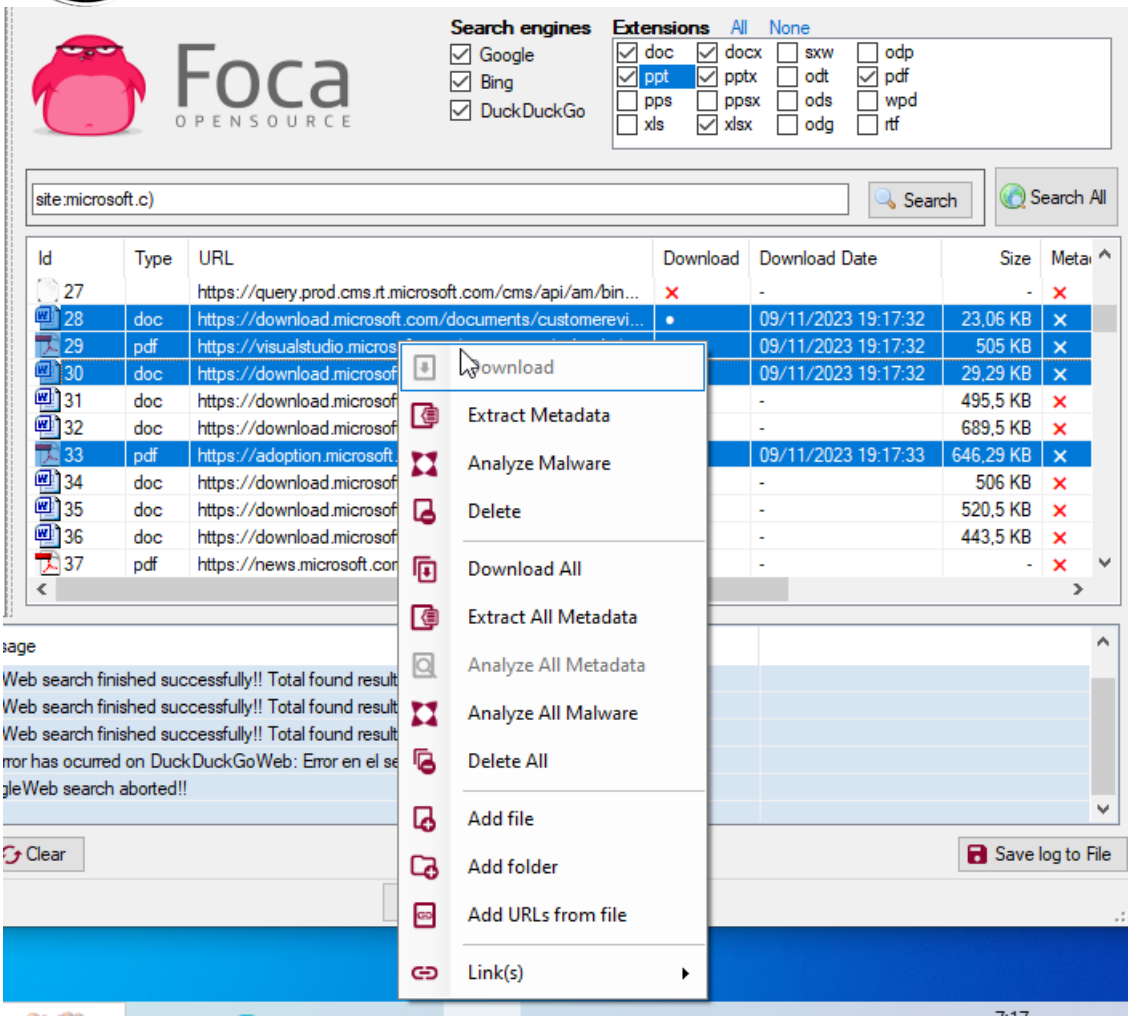

TaskList
About
Foca
OPENSOURCE
Select project
Project name
Project of microsoft.com
Domain website
microsoft.com
Alternative domains
Folder where to save documents
C:\Users\vboxuser\AppData\Local\T
Project date
lunes , 11 de septiembre de 2023
Project notes
Create
Import
Cancel

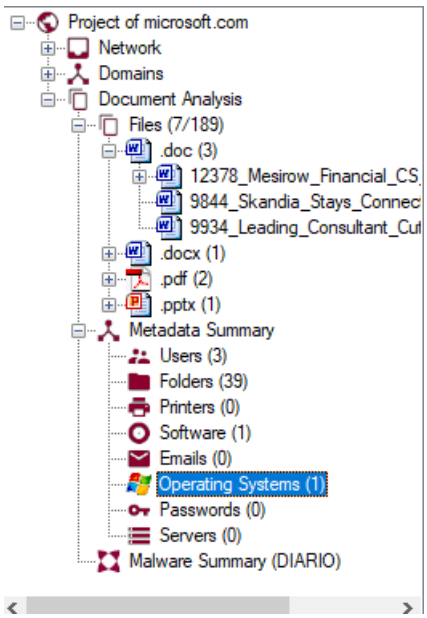

Project of microsoft.com - FOCA Open Source 3.4.7.1
Project
Plugins
Options
TaskList
About
Project of microsoft.com
Network
Domains
Document Analysis
Foca
OPENSOURCE
Search engines
Google
Bing
DuckDuckGo
Extensions
All
None
doc
docx
sxw
odp
ppt
pptx
odt
pdf
pps
ppsx
ods
wpd
xls
xlsx
odg
rtf
Custom search
Search All
Id
Type
URL
Download
Download Date
Size
Metadata
Project of microsoft.com - FOCA Open Source 3.4.7.1
Project saved successfully!
Aceptar
Time
Source
Severity
Message
Settings
Deactivate AutoScroll
Clear
Save log to File



11. Seleccionar los resultados y hacer la extracción de metadata



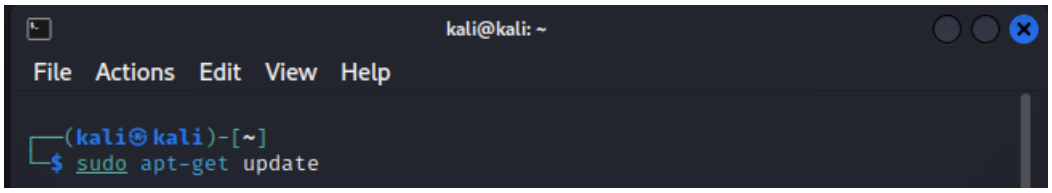

Foca
OPENSOURCE
Search engines
Google
Bing
DuckDuckGo
Extensions
All
None
doc
docx
sxw
odp
ppt
pptx
odt
pdf
pps
ppsx
ods
wpd
xls
xlsx
odg
rtf
site:microsoft.c)
Search
Search All
Id
Type
URL
Download
Download Date
Size
27
28 doc https://download.microsoft.com/documents/customerevi... 09/11/2023 19:17:32 23,06 KB
29 pdf https://visualstudio.micros 09/11/2023 19:17:32 505 KB
30 doc https://download.microsof 09/11/2023 19:17:32 29,29 KB
31 doc https://download.microsof 495,5 KB
32 doc https://download.microsof 689,5 KB
33 pdf https://adoption.microsoft. 09/11/2023 19:17:33 646,29 KB
34 doc https://download.microsof 506 KB
35 doc https://download.microsof 520,5 KB
36 doc https://download.microsof 443,5 KB
37 pdf https://news.microsoft.cor
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)
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
gleWeb search aborted!!
Clear
Save log to File


Project of microsoft.com
Network
Domains
Document Analysis
Files (7/189)
.doc (3)
12378_Mesirow_Financial_CS
9844_Skandia_Stays_Connec
9934_Leading_Consultant_Cul
.docx (1)
.pdf (2)
.pptx (1)
Metadata Summary
Users (3)
Folders (39)
Printers (0)
Software (1)
Emails (0)
Operating Systems (1)
Passwords (0)
Servers (0)
Malware Summary (DIARIO)

METAGOOFIL

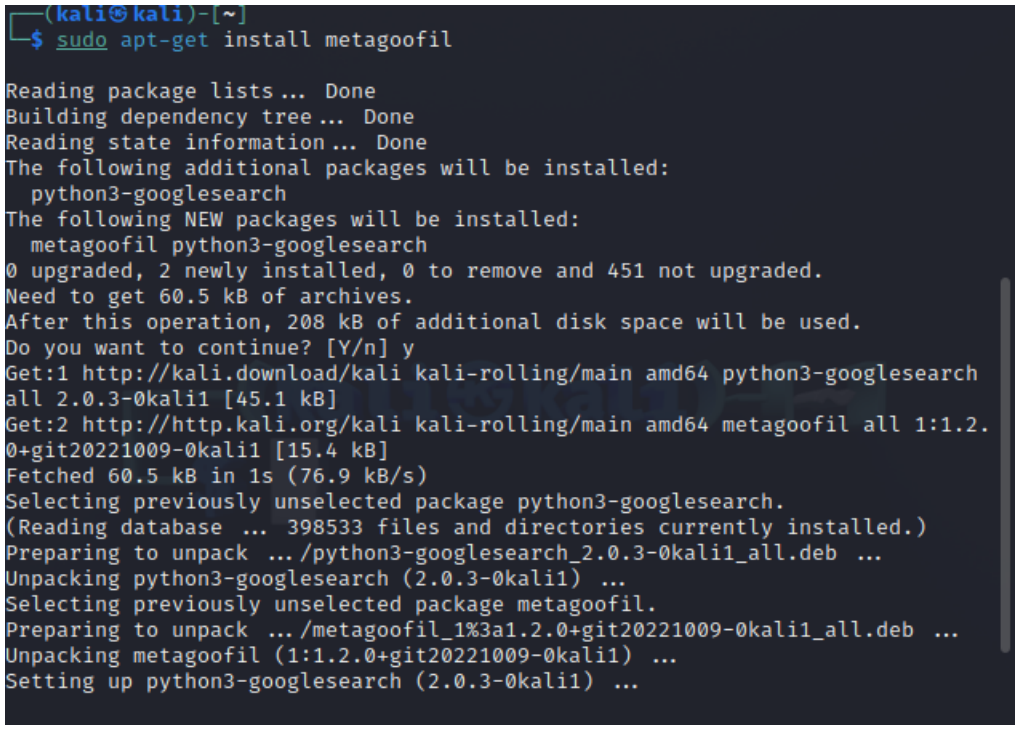
1. Actualizar el Kali con un

sudo apt-get update



2. Instalamos el metagoofil

sudo apt-get install metagoofil



3. metagoofil -h

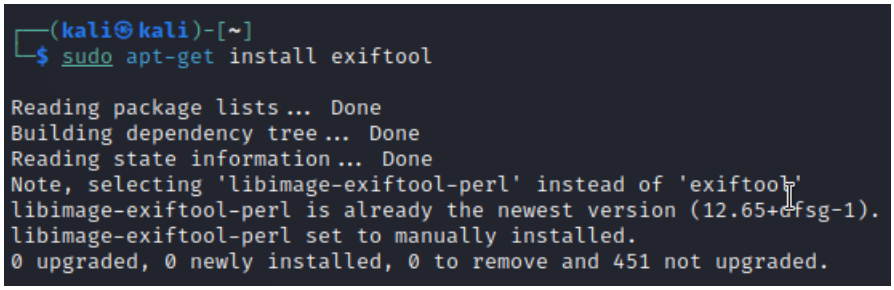
```
┌──(kali㉿kali)-[~]
└─$ metagoofil -h
usage: metagoofil.py [-h] -d DOMAIN [-e DELAY] [-f [SAVE_FILE]]
                     [-i URL_TIMEOUT] [-l SEARCH_MAX]
                     [-n DOWNLOAD_FILE_LIMIT] [-o SAVE_DIRECTORY]
                     [-r NUMBER_OF_THREADS] -t FILE_TYPES [-u [USER_AGENT]]
                     [-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 microsft.com -l 10 -t pdf,doc,ppt -o Desktop
[*] Searching for 10 .pdf files and waiting 30.0 seconds between searches
```

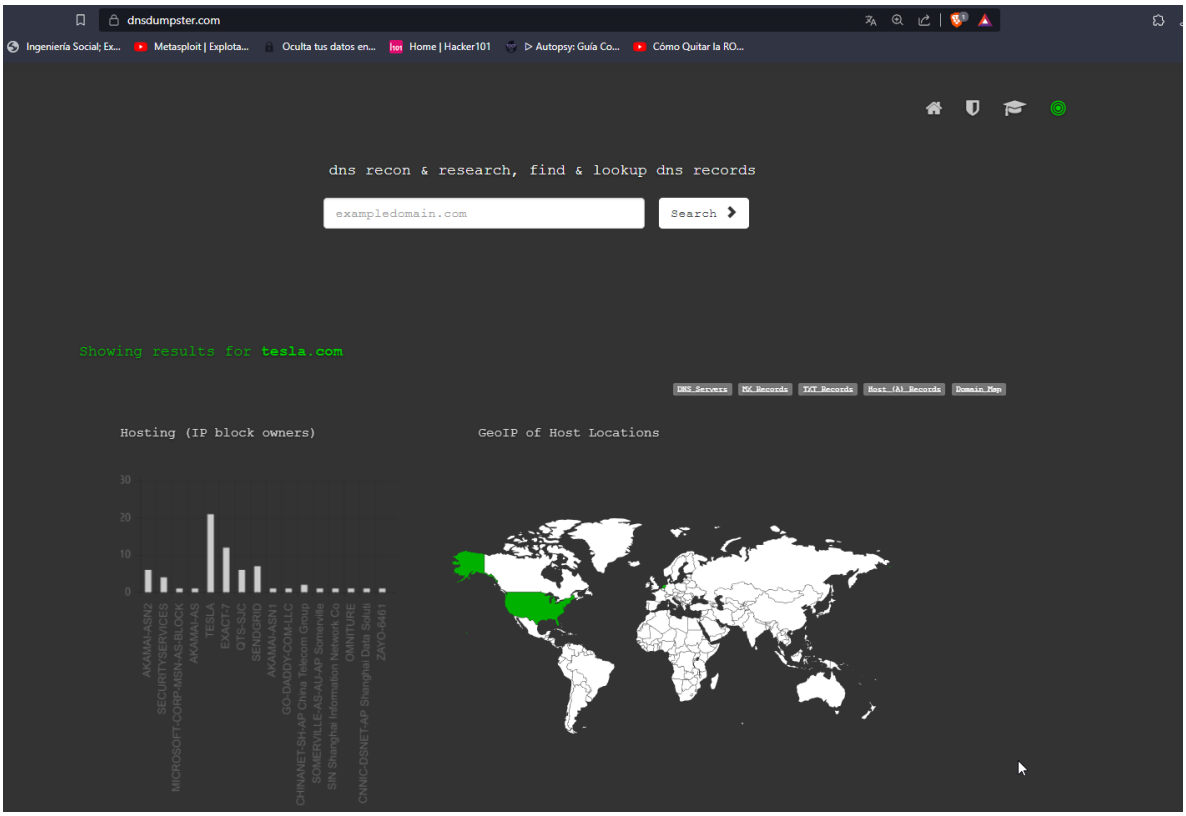
4. para poder ver los metadatos hay que insyalar una utilidad

sudo apt-get imnstall exiftool



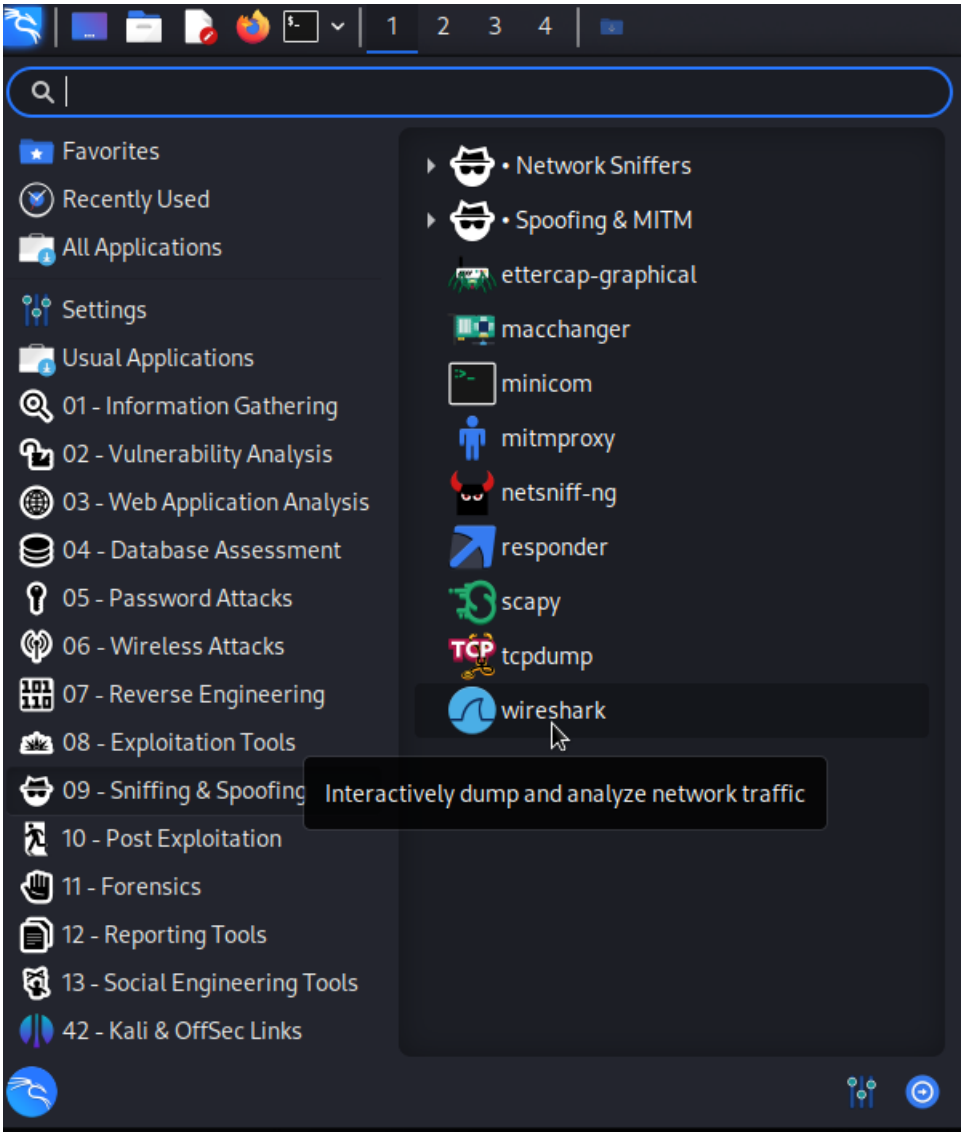
Exiftool -r *.pdf | egrep -i “Author|Creator|Email| Producer | Template” | sort -u

DNS DUMPSTER

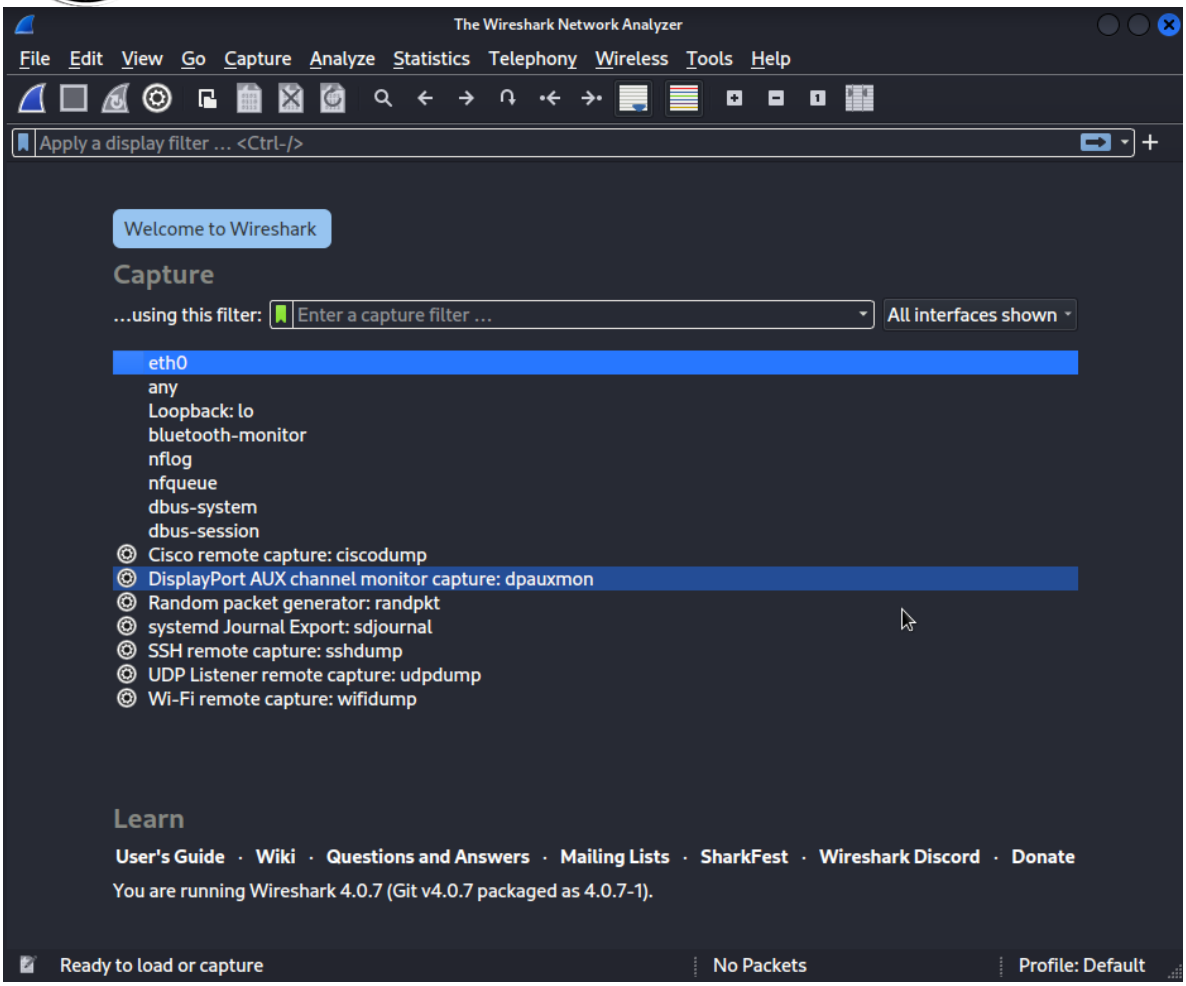


SNIFFERS:WIRESHARK

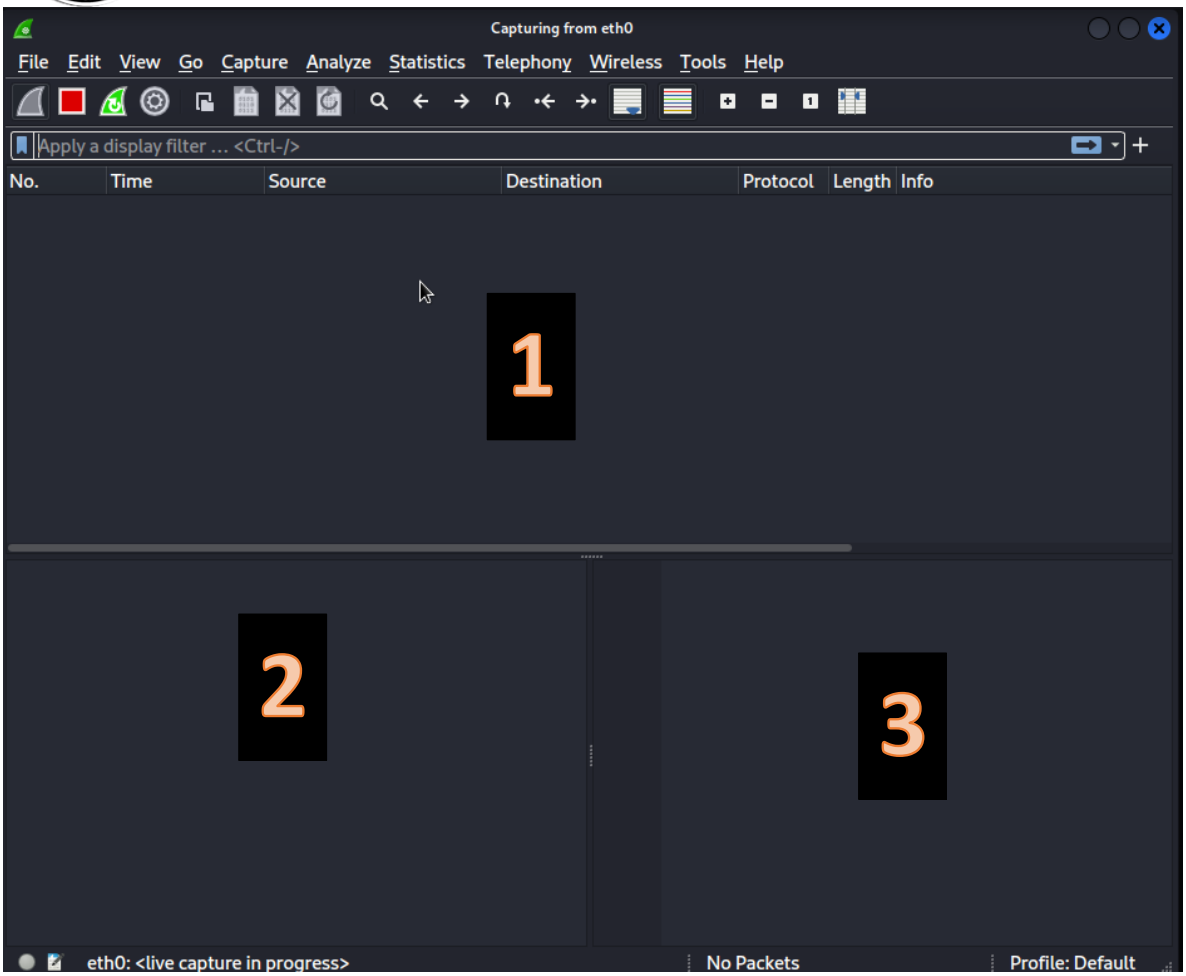
1. ingresar a wireshark

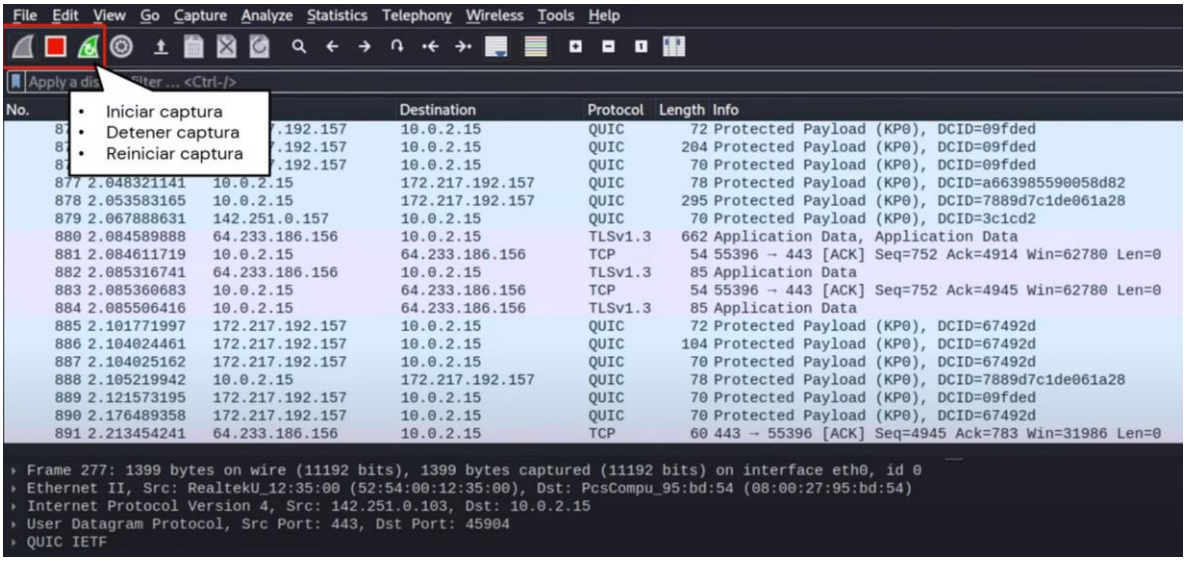


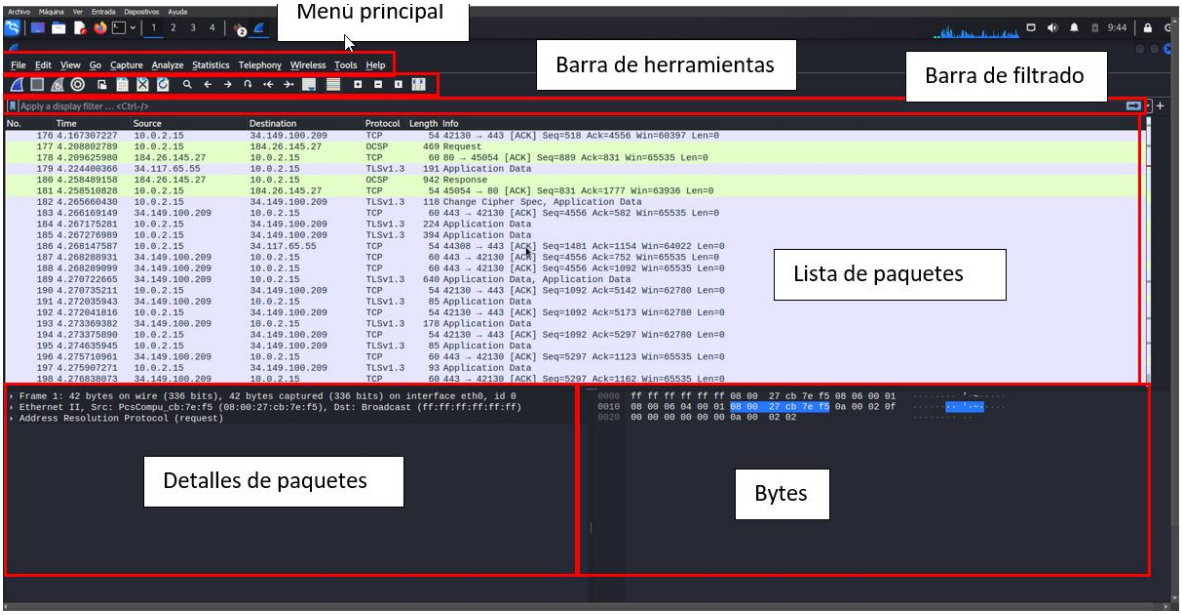
2. conociendo la interfaz



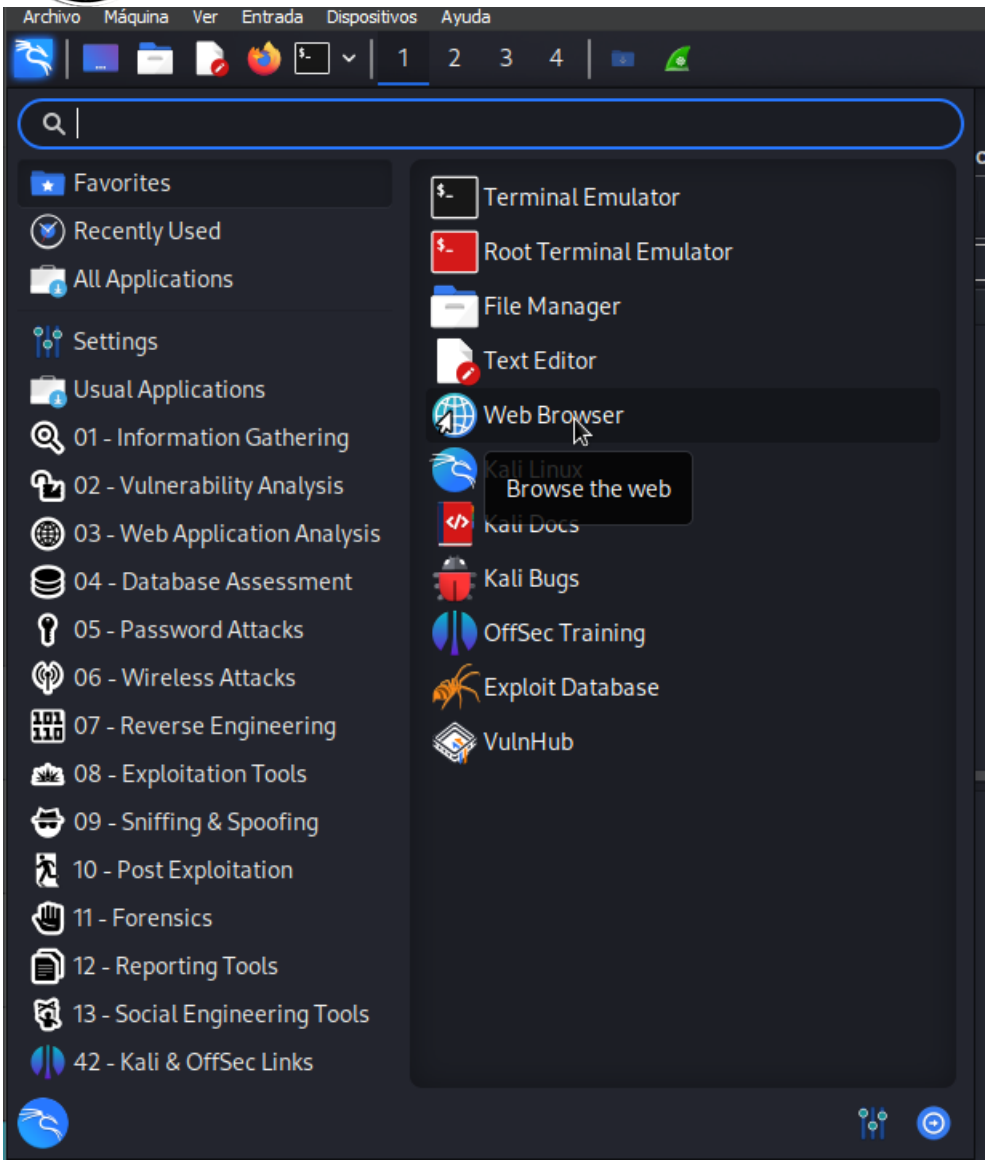
3. Dar doble clic en cualquier interfaz en este caso la que nos interesa es la eth0

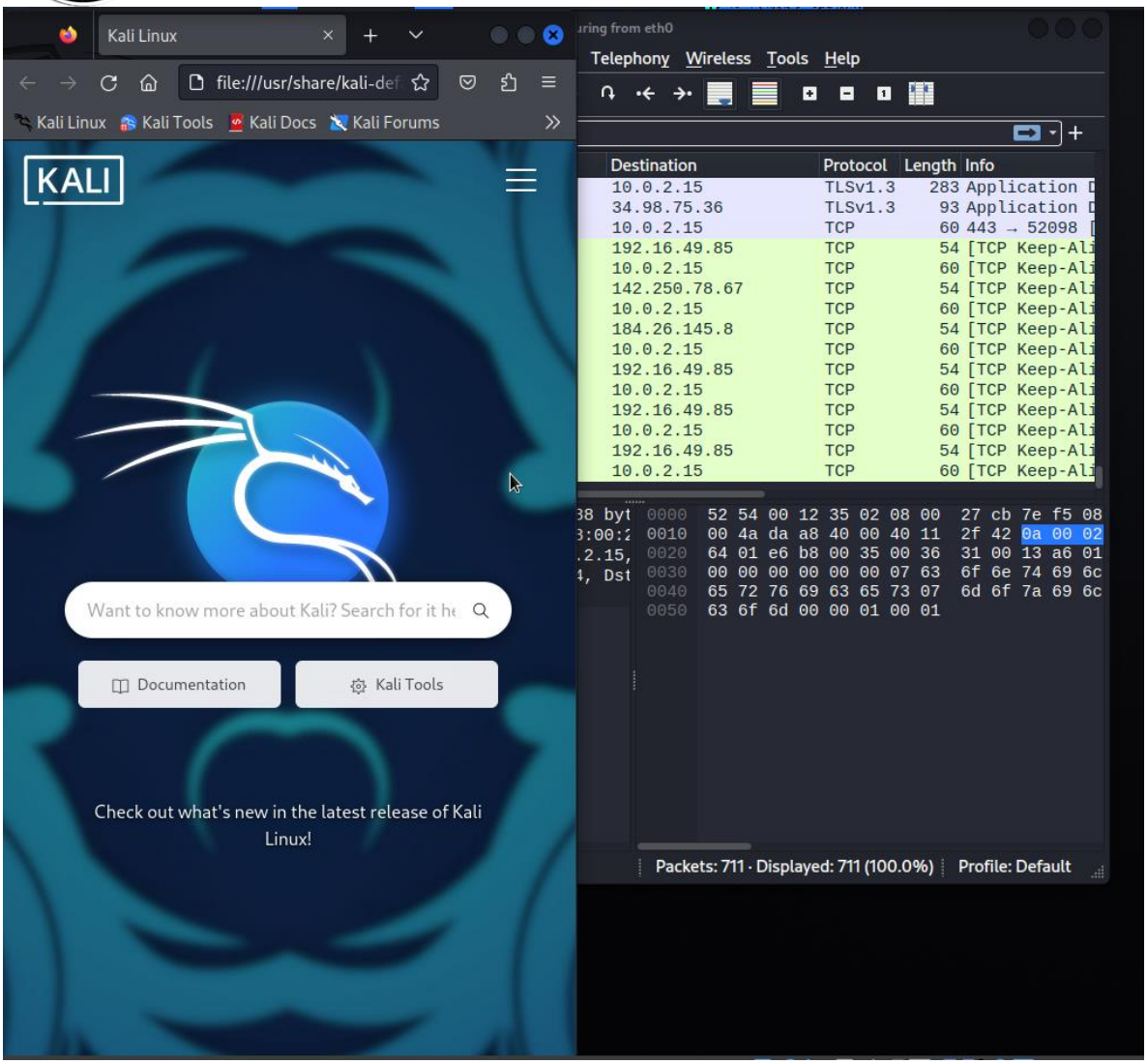

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1
2
3
eth0: <live capture in progress>
No Packets
Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Iniciar captura
Detener captura
Reiniciar captura
No. Destination Protocol Length Info
877 2.048321141 10.0.2.15 172.217.192.157 QUIC 78 Protected Payload (KP0), DCID=a663985590058d82
878 2.053583165 10.0.2.15 172.217.192.157 QUIC 295 Protected Payload (KP0), DCID=7889d7c1de061a28
879 2.067888631 142.251.0.157 10.0.2.15 QUIC 70 Protected Payload (KP0), 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 (KP0), DCID=67492d
886 2.104024461 172.217.192.157 10.0.2.15 QUIC 104 Protected Payload (KP0), DCID=67492d
887 2.104025162 172.217.192.157 10.0.2.15 QUIC 70 Protected Payload (KP0), DCID=67492d
888 2.105219942 10.0.2.15 172.217.192.157 QUIC 78 Protected Payload (KP0), DCID=7889d7c1de061a28
889 2.121573195 172.217.192.157 10.0.2.15 QUIC 70 Protected Payload (KP0), DCID=09fded
890 2.176489358 172.217.192.157 10.0.2.15 QUIC 70 Protected Payload (KP0), 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

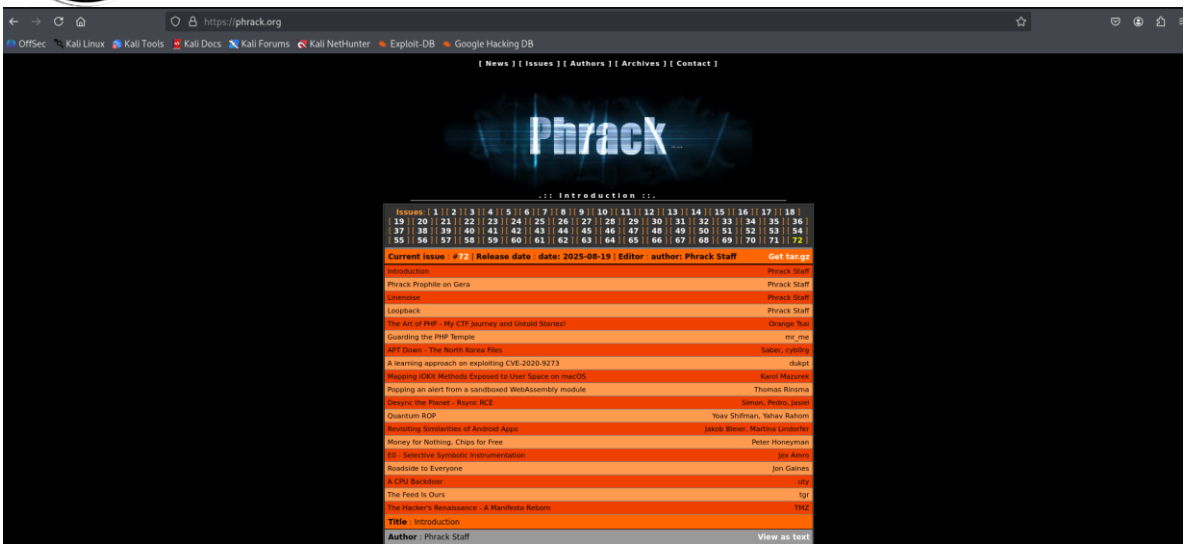


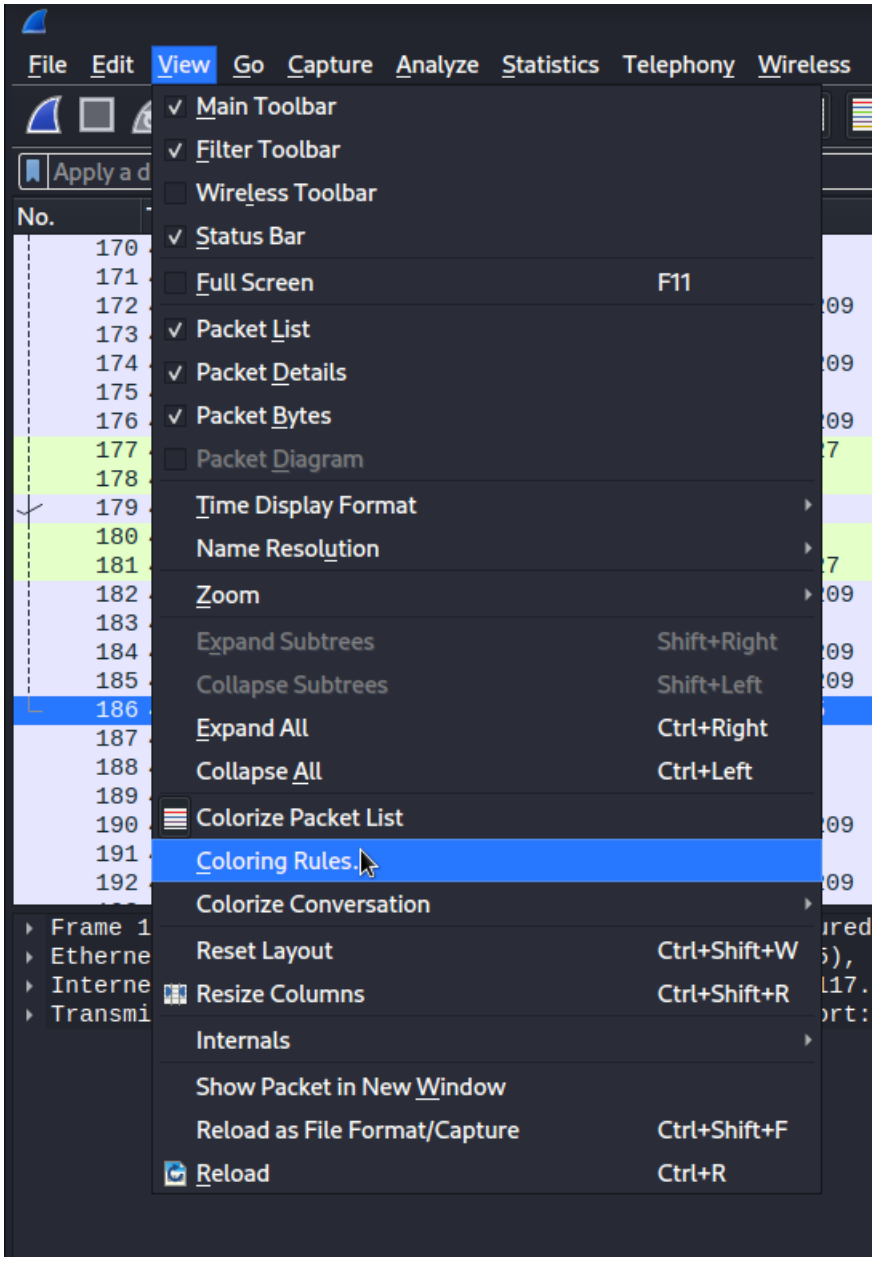
4. General trafico de red

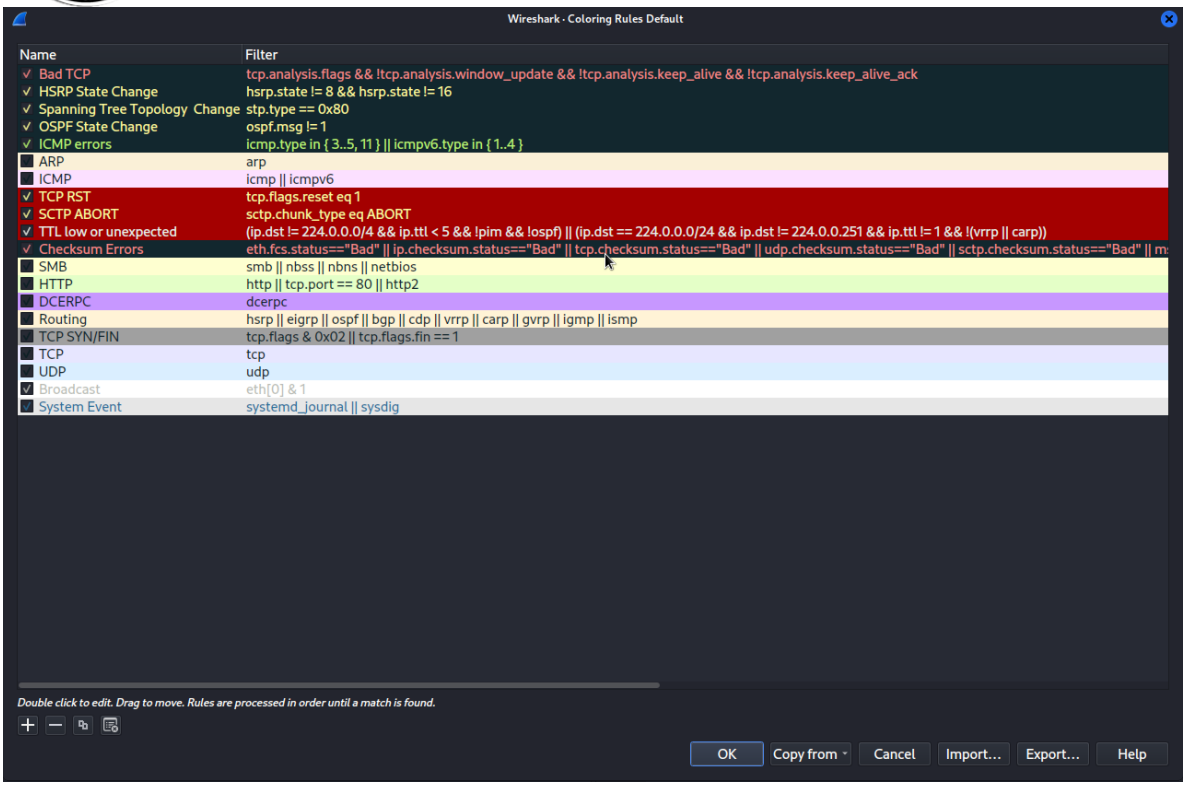

Archivo
Máquina
Ver
Entrada
Dispositivos
Ayuda
1
2
3
4
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
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
Browse the web
Kali Bugs
OffSec Training
Exploit Database
VulnHub



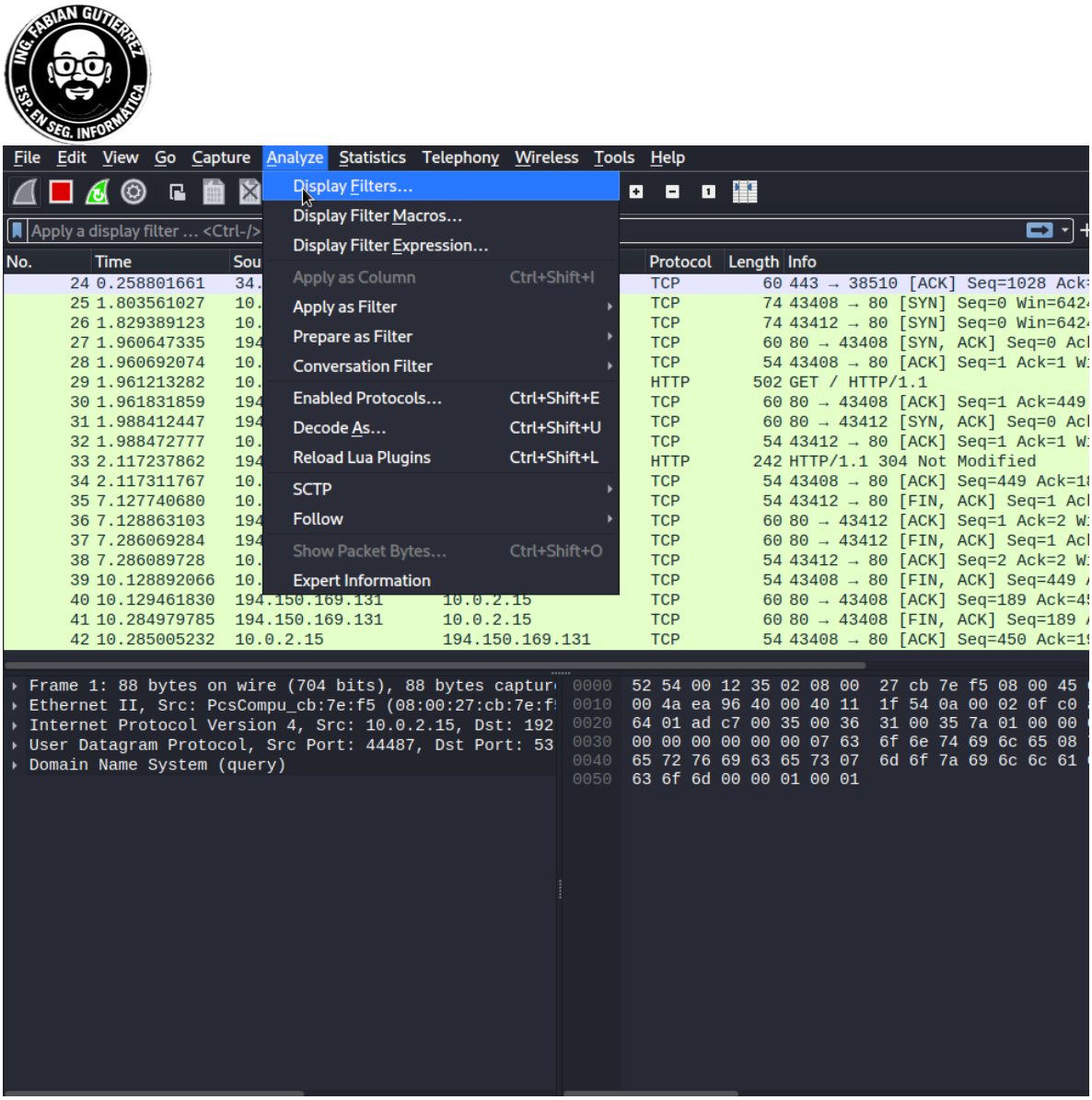
Ingresar a phrack.org

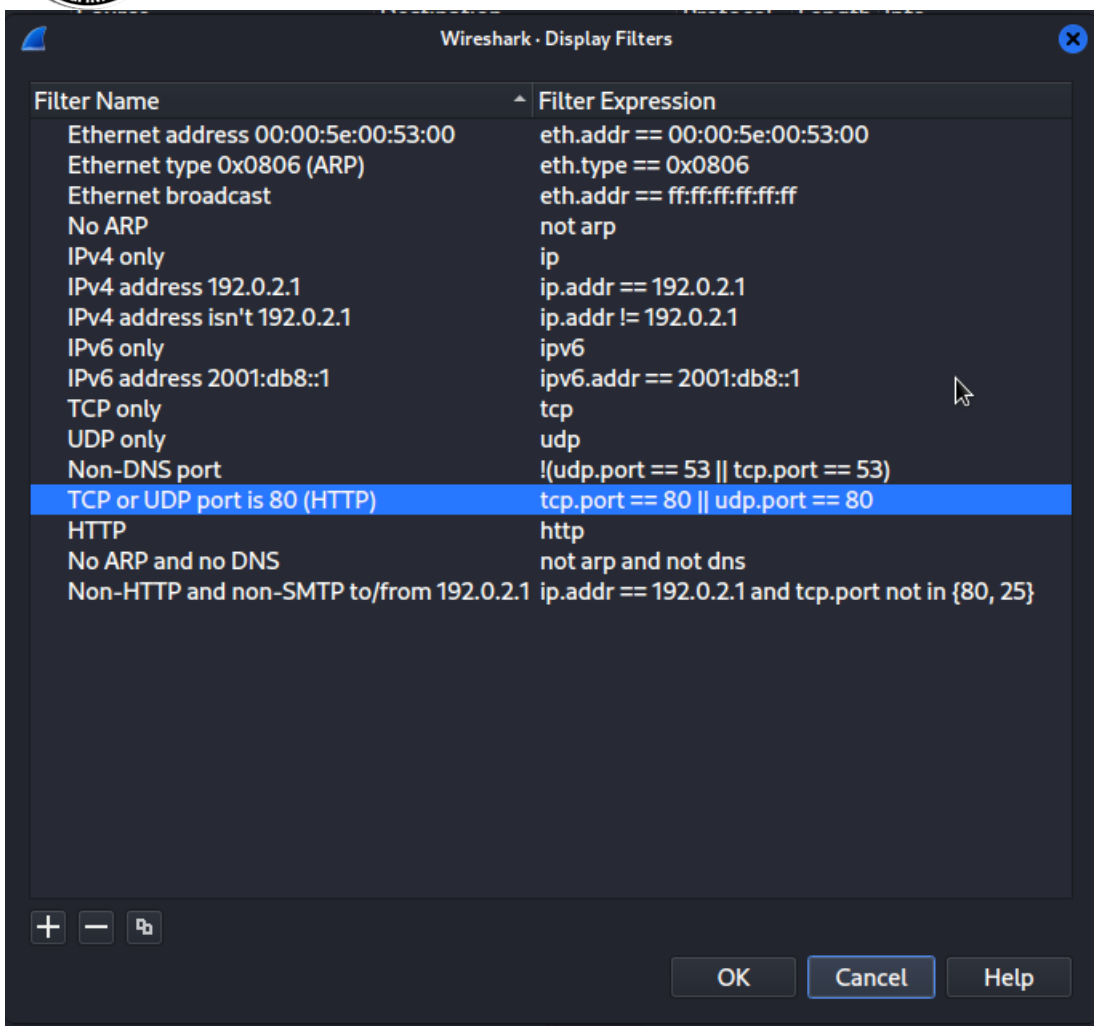

https://phrack.org
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
[News] [Issues] [Authors] [Archives] [Contact]
Phrack
.:: Introduction ::.
Issues [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [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 Prophile on Gera Phrack Staff
Linenoise Phrack Staff
Loopback Phrack Staff
The Art of PHP - My CTF Journey and Untold Stories! Orange Tsai
Guarding the PHP Temple mr_me
APT Down - The North Korea Files Saber, cyb0rg
A learning approach on exploiting CVE-2020-9273 dukpt
Mapping IOKit Methods Exposed to User Space on macOS Karol Mazurek
Popping an alert from a sandboxed WebAssembly module Thomas Rinsma
Desync the Planet - Rsync RCE Simon, Pedro, Jasiel
Quantum ROP Yoav Shifman, Yahav Rahom
Revisiting Similarities of Android Apps Jakob Bleier, Martina Lindorfer
Money for Nothing, Chips for Free Peter Honeyman
ES - Selective Symbolic Instrumentation Jex Amro
Roadside to Everyone Jon Gaines
A CPU Backdoor uty
The Feed Is Ours tgr
The Hacker's Renaissance - A Manifesto Reborn TMZ
Title : Introduction
Author : Phrack Staff
View as text

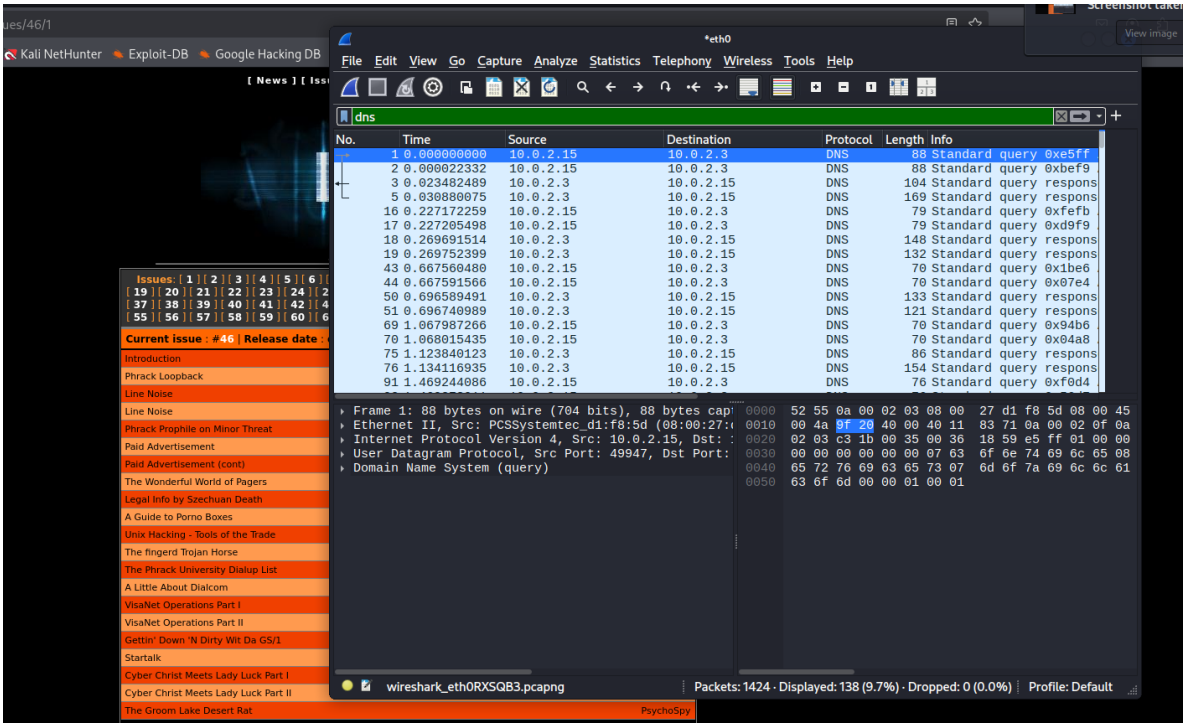

File Edit View Go Capture Analyze Statistics Telephony Wireless
Main Toolbar
Filter Toolbar
Wireless Toolbar
Status Bar
Full Screen F11
Packet List
Packet Details
Packet Bytes
Packet Diagram
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout Ctrl+Shift+W
Resize Columns Ctrl+Shift+R
Internals
Show Packet in New Window
Reload as File Format/Capture Ctrl+Shift+F
Reload Ctrl+R
No.
Frame 1
Etherne
Interne
Transmi

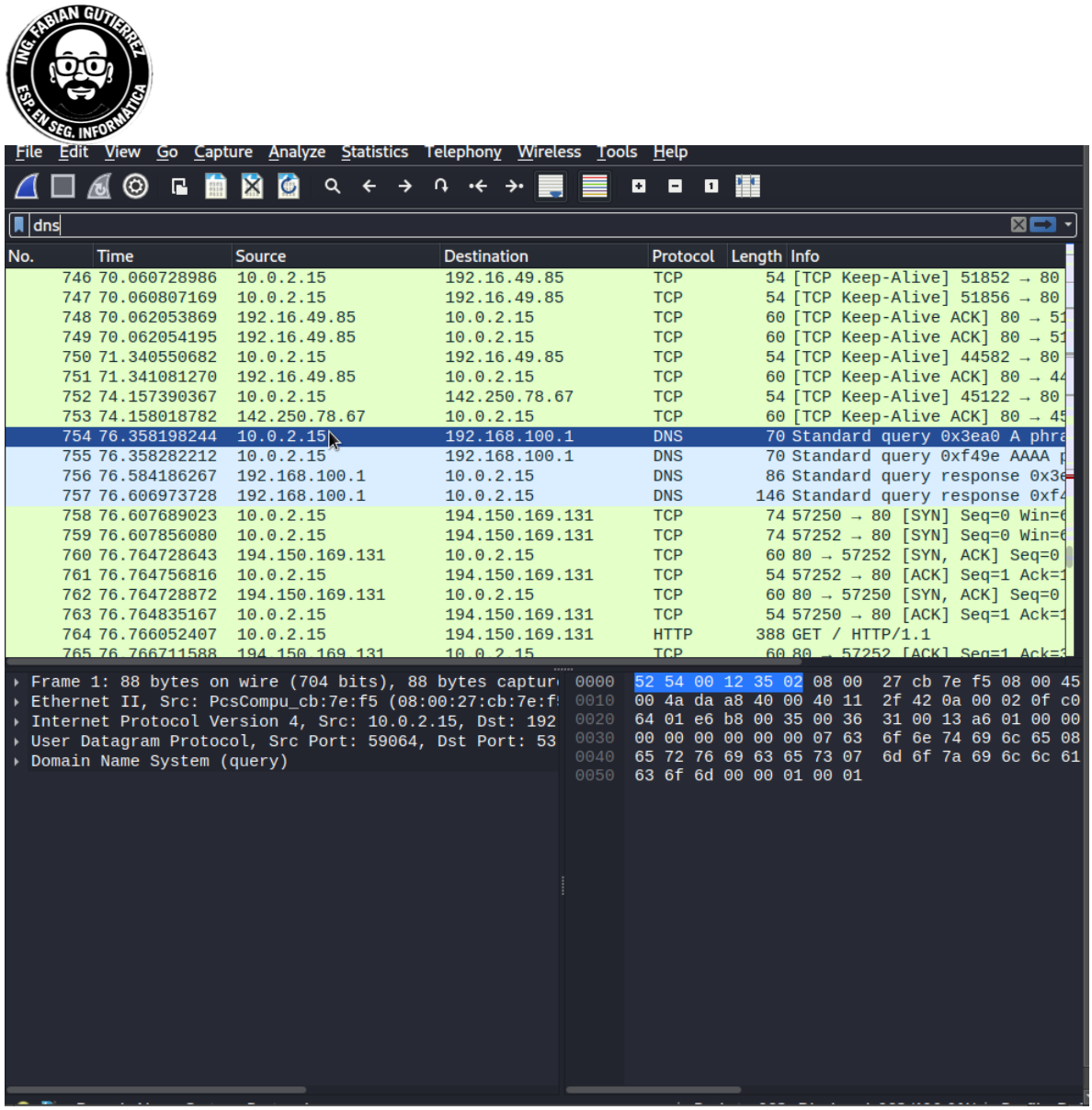

Wireshark · Coloring Rules Default
Name
Filter
Bad TCP
tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
HSRP State Change
hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 1
ICMP 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 != 224.0.0.0/4 && ip.ttl < 5 && !pim && !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" || m
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

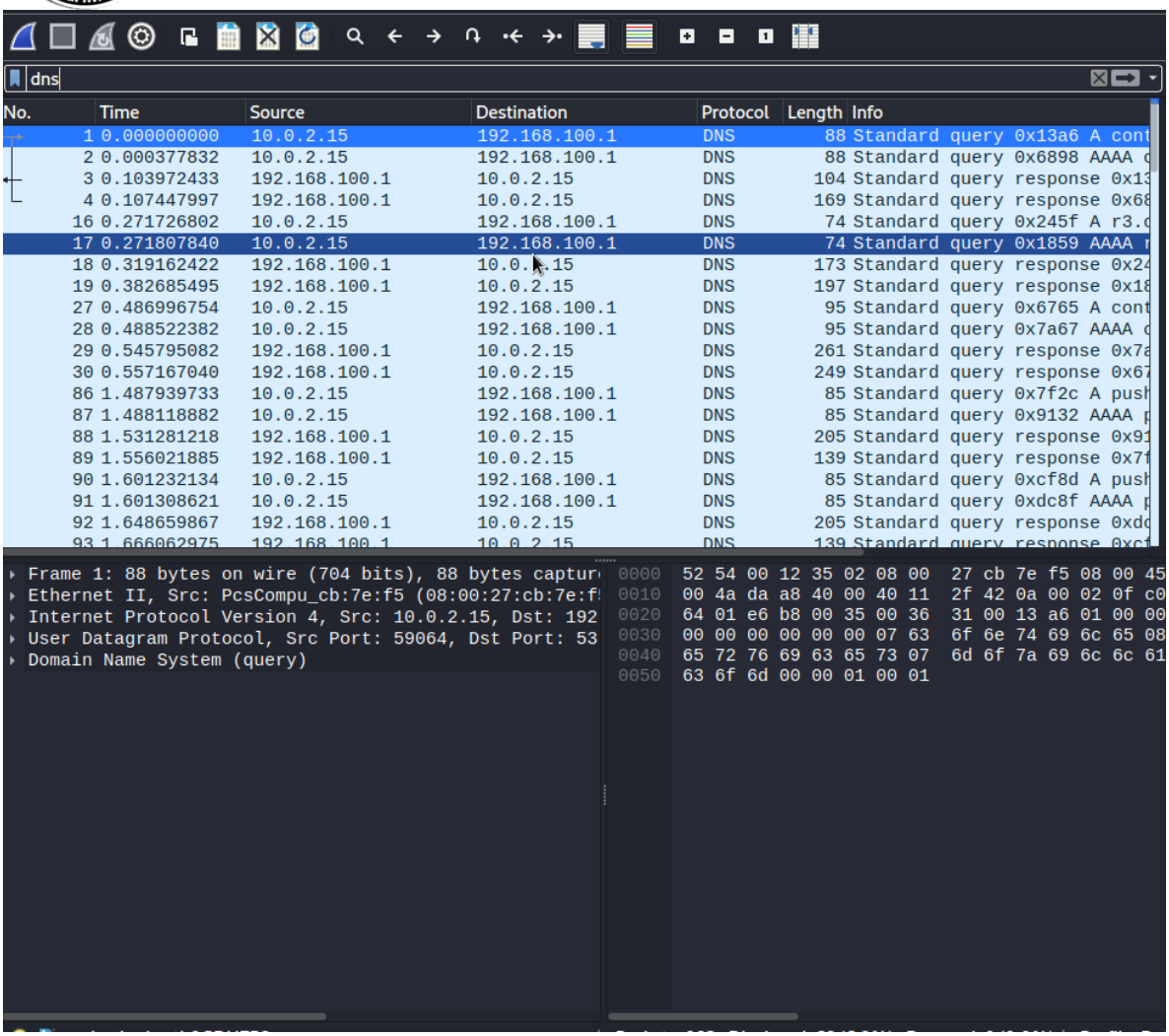
5. Filtrado


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Display Filters...
Display Filter Macros...
Display Filter Expression...
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Enabled Protocols... Ctrl+Shift+E
Decode As... Ctrl+Shift+U
Reload Lua Plugins Ctrl+Shift+L
SCTP
Follow
Show Packet Bytes... Ctrl+Shift+O
Expert Information
Apply a display filter ... <Ctrl-/>
No. Time Sou Protocol Length Info
24 0.258801661 34. TCP 60 443 → 38510 [ACK] Seq=1028 Ack
25 1.803561027 10. TCP 74 43408 → 80 [SYN] Seq=0 Win=642
26 1.829389123 10. TCP 74 43412 → 80 [SYN] Seq=0 Win=642
27 1.960647335 194 TCP 60 80 → 43408 [SYN, ACK] Seq=0 Ac
28 1.960692074 10. TCP 54 43408 → 80 [ACK] Seq=1 Ack=1 W
29 1.961213282 10. HTTP 502 GET / HTTP/1.1
30 1.961831859 194 TCP 60 80 → 43408 [ACK] Seq=1 Ack=449
31 1.988412447 194 TCP 60 80 → 43412 [SYN, ACK] Seq=0 Ac
32 1.988472777 10. TCP 54 43412 → 80 [ACK] Seq=1 Ack=1 W
33 2.117237862 194 HTTP 242 HTTP/1.1 304 Not Modified
34 2.117311767 10. TCP 54 43408 → 80 [ACK] Seq=449 Ack=1
35 7.127740680 10. TCP 54 43412 → 80 [FIN, ACK] Seq=1 Ac
36 7.128863103 194 TCP 60 80 → 43412 [ACK] Seq=1 Ack=2 W
37 7.286069284 194 TCP 60 80 → 43412 [FIN, ACK] Seq=1 Ac
38 7.286089728 10. TCP 54 43412 → 80 [ACK] Seq=2 Ack=2 W
39 10.128892066 10. TCP 54 43408 → 80 [FIN, ACK] Seq=449
40 10.129461830 194.150.169.131 10.0.2.15 TCP 60 80 → 43408 [ACK] Seq=189 Ack=4
41 10.284979785 194.150.169.131 10.0.2.15 TCP 60 80 → 43408 [FIN, ACK] Seq=189
42 10.285005232 10.0.2.15 194.150.169.131 TCP 54 43408 → 80 [ACK] Seq=450 Ack=1
Frame 1: 88 bytes on wire (704 bits), 88 bytes captur
Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192
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
0010 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

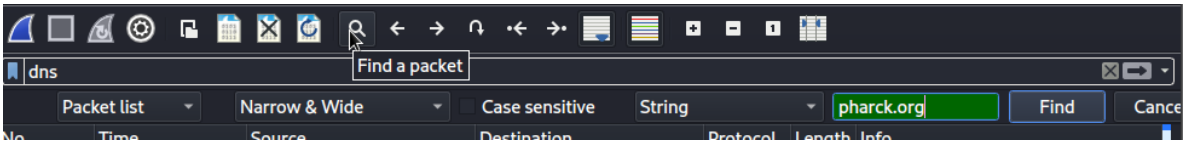

Wireshark · Display Filters
Filter Name
Filter Expression
Ethernet address 00:00:5e:00:53:00
eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)
eth.type == 0x0806
Ethernet broadcast
eth.addr == ff:ff:ff:ff:ff:ff
No ARP
not arp
IPv4 only
ip
IPv4 address 192.0.2.1
ip.addr == 192.0.2.1
IPv4 address 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

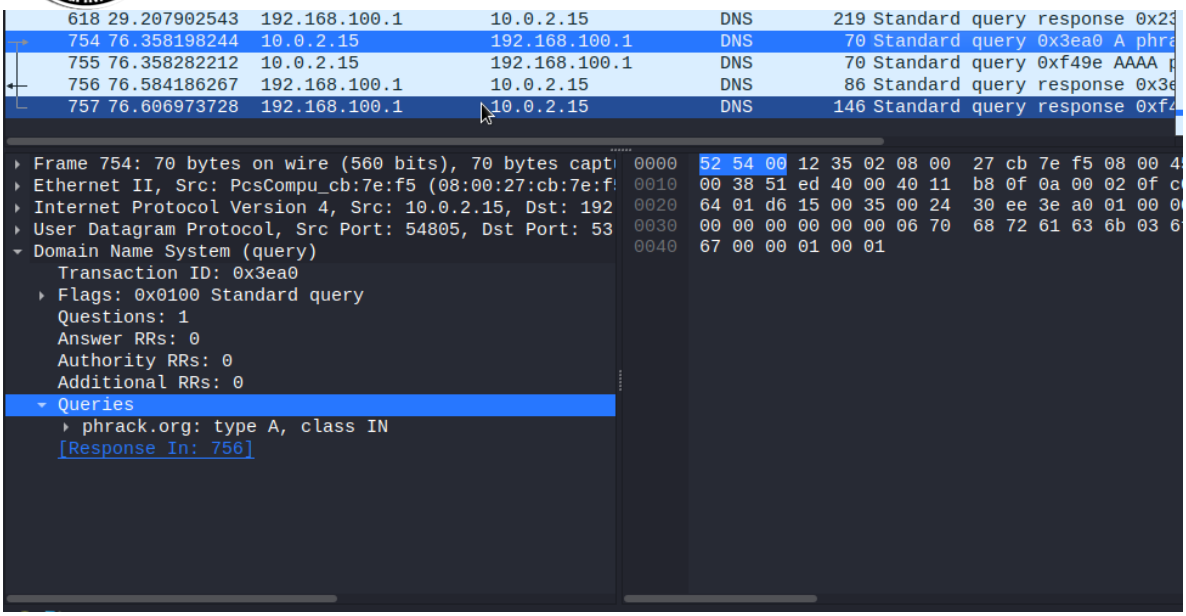

Kali NetHunter
Exploit-DB
Google Hacking DB
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
1 0.000000000 10.0.2.15 10.0.2.3 DNS 88 Standard query 0xe5ff
2 0.000022332 10.0.2.15 10.0.2.3 DNS 88 Standard query 0xbef9
3 0.023482489 10.0.2.3 10.0.2.15 DNS 104 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 0xfefb
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 0.667591566 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 1.469244086 10.0.2.15 10.0.2.3 DNS 76 Standard query 0xf0d4
Frame 1: 88 bytes on wire (704 bits), 88 bytes cap
Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:
Internet Protocol Version 4, Src: 10.0.2.15, Dst:
User Datagram Protocol, Src Port: 49947, Dst Port:
Domain Name System (query)
0000 52 55 0a 00 02 03 08 00 27 d1 f8 5d 08 00 45
0010 00 4a 9f 20 40 00 40 11 83 71 0a 00 02 0f 0a
0020 02 03 c3 1b 00 35 00 36 18 59 e5 ff 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_eth0RXSQB3.pcapng
Packets: 1424 · Displayed: 138 (9.7%) · Dropped: 0 (0.0%)
Profile: Default
Issues: [1] [2] [3] [4] [5] [6]
[19] [20] [21] [22] [23] [24]
[37] [38] [39] [40] [41] [42]
[55] [56] [57] [58] [59] [60]
Current issue : #46 | Release date :
Introduction
Phrack Loopback
Line Noise
Line Noise
Phrack Prophile on Minor Threat
Paid Advertisement
Paid Advertisement (cont)
The Wonderful World of Pagers
Legal Info by Szechuan Death
A Guide to Porno Boxes
Unix Hacking - Tools of the Trade
The fingerd Trojan Horse
The Phrack University Dialup List
A Little About Dialcom
VisaNet Operations Part I
VisaNet Operations Part II
Gettin' Down 'N Dirty Wit Da GS/1
Startalk
Cyber Christ Meets Lady Luck Part I
Cyber Christ Meets Lady Luck Part II
The Groom Lake Desert Rat
PsychoSpy


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
746 70.060728986 10.0.2.15 192.16.49.85 TCP 54 [TCP Keep-Alive] 51852 → 80
747 70.060807169 10.0.2.15 192.16.49.85 TCP 54 [TCP Keep-Alive] 51856 → 80
748 70.062053869 192.16.49.85 10.0.2.15 TCP 60 [TCP Keep-Alive ACK] 80 → 51
749 70.062054195 192.16.49.85 10.0.2.15 TCP 60 [TCP Keep-Alive ACK] 80 → 51
750 71.340550682 10.0.2.15 192.16.49.85 TCP 54 [TCP Keep-Alive] 44582 → 80
751 71.341081270 192.16.49.85 10.0.2.15 TCP 60 [TCP Keep-Alive ACK] 80 → 44
752 74.157390367 10.0.2.15 142.250.78.67 TCP 54 [TCP Keep-Alive] 45122 → 80
753 74.158018782 142.250.78.67 10.0.2.15 TCP 60 [TCP Keep-Alive ACK] 80 → 45
754 76.358198244 10.0.2.15 192.168.100.1 DNS 70 Standard query 0x3ea0 A phra
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
758 76.607689023 10.0.2.15 194.150.169.131 TCP 74 57250 → 80 [SYN] Seq=0 Win=6
759 76.607856080 10.0.2.15 194.150.169.131 TCP 74 57252 → 80 [SYN] Seq=0 Win=6
760 76.764728643 194.150.169.131 10.0.2.15 TCP 60 80 → 57252 [SYN, ACK] Seq=0
761 76.764756816 10.0.2.15 194.150.169.131 TCP 54 57252 → 80 [ACK] Seq=1 Ack=1
762 76.764728872 194.150.169.131 10.0.2.15 TCP 60 80 → 57250 [SYN, ACK] Seq=0
763 76.764835167 10.0.2.15 194.150.169.131 TCP 54 57250 → 80 [ACK] Seq=1 Ack=1
764 76.766052407 10.0.2.15 194.150.169.131 HTTP 388 GET / HTTP/1.1
765 76.766711588 194.150.169.131 10.0.2.15 TCP 60 80 → 57252 [ACK] Seq=1 Ack=3
Frame 1: 88 bytes on wire (704 bits), 88 bytes captur
Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192
User Datagram Protocol, Src Port: 59064, Dst Port: 53
Domain Name System (query)
0000 52 54 00 12 35 02 08 00 27 cb 7e f5 08 00 45
0010 00 4a da a8 40 00 40 11 2f 42 0a 00 02 0f c0
0020 64 01 e6 b8 00 35 00 36 31 00 13 a6 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

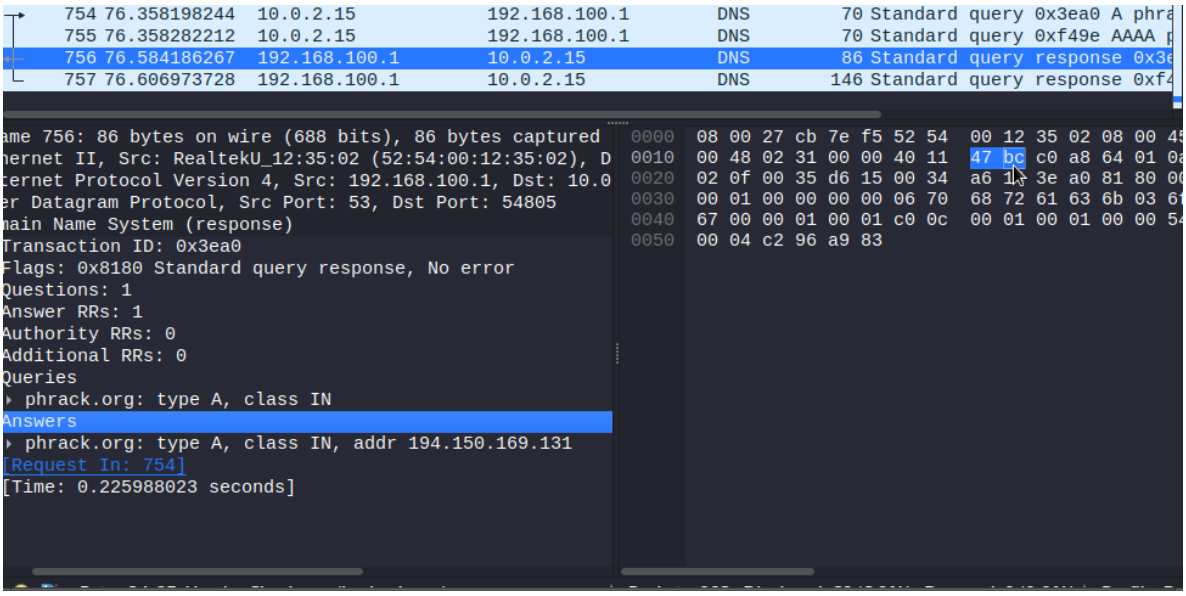


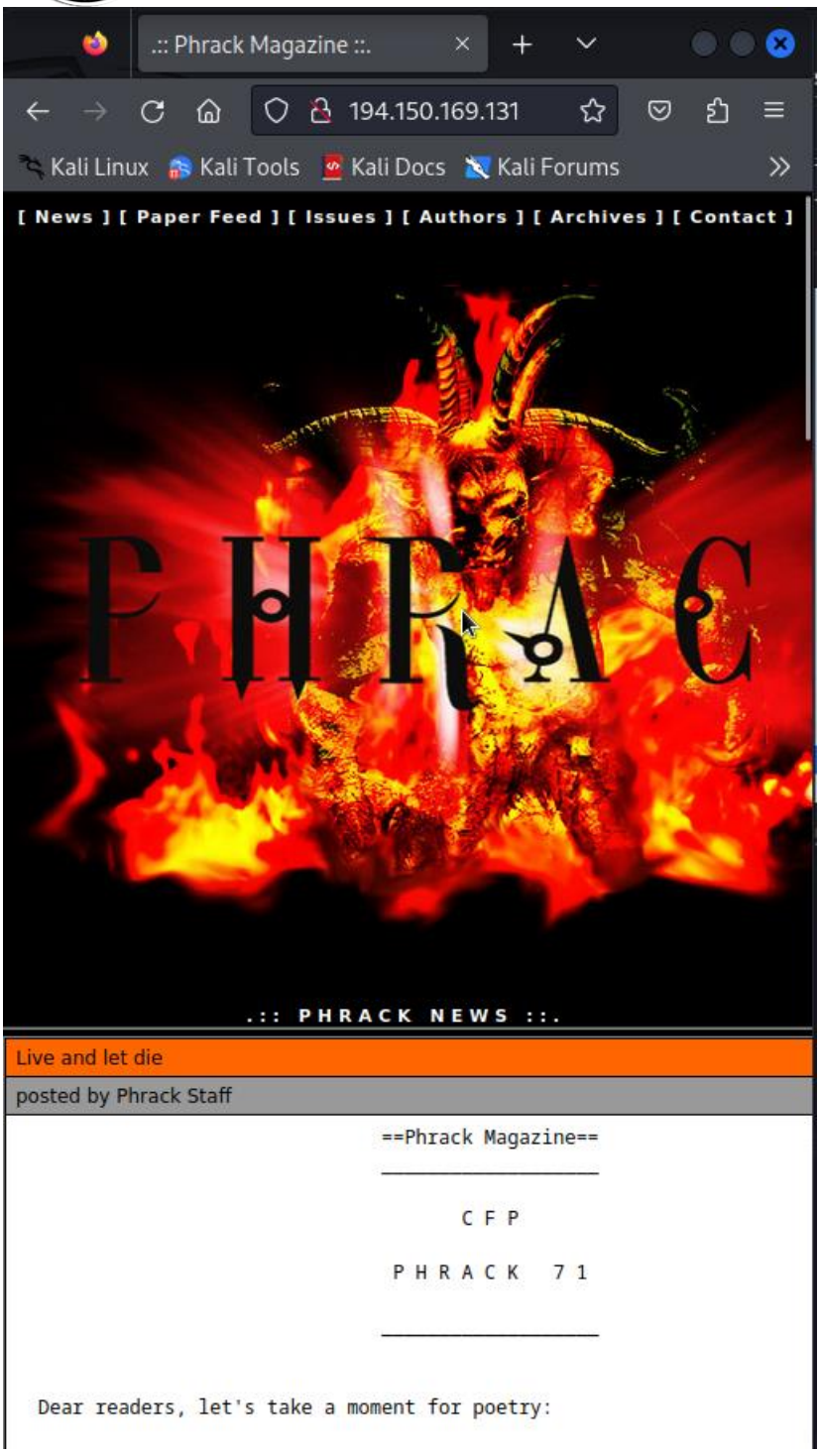
Vamos a buscar un string





Todo petición debe tener una respuesta

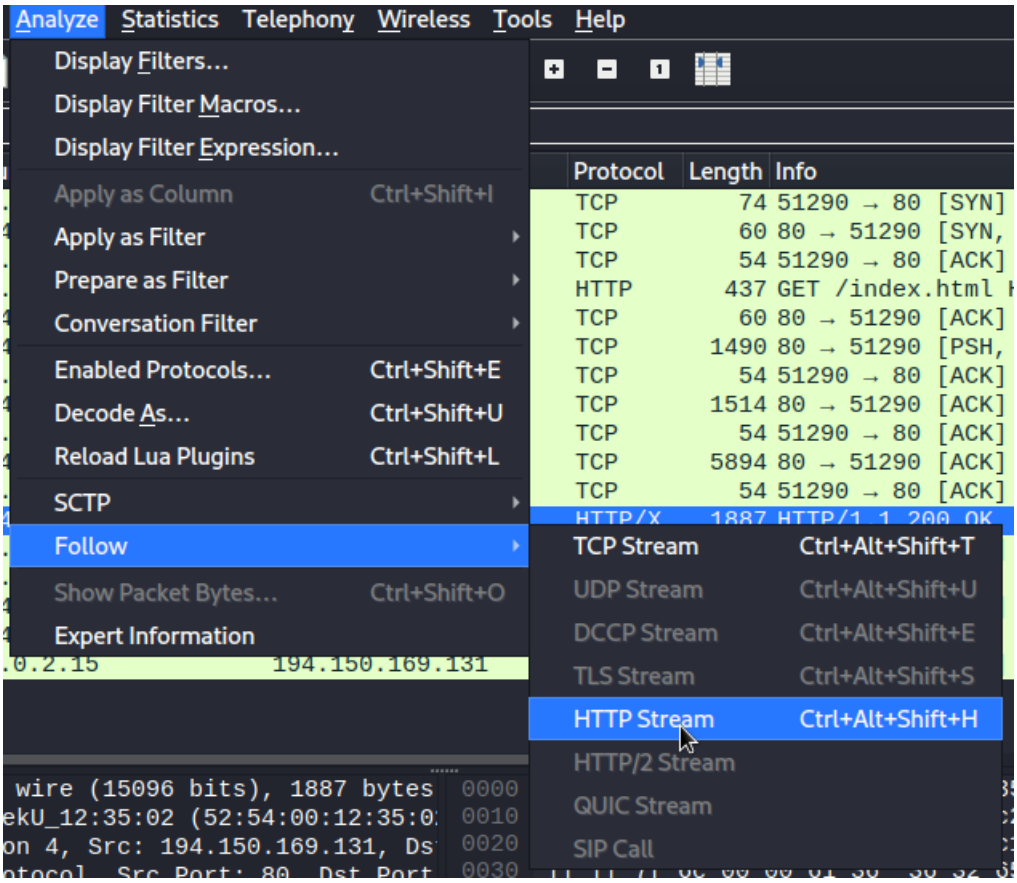


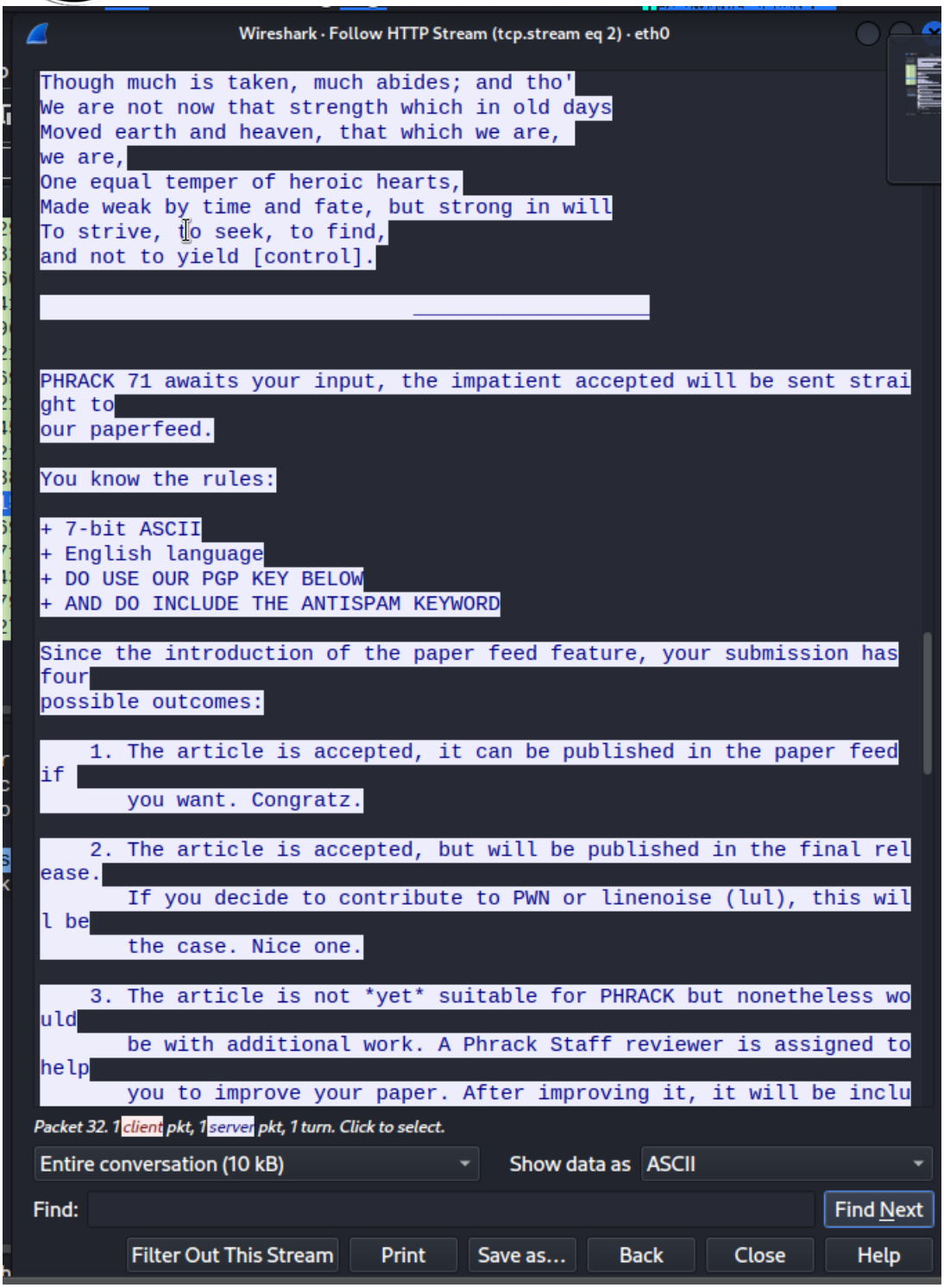

.:: Phrack Magazine ::.
194.150.169.131
Kali Linux
Kali Tools
Kali Docs
Kali Forums
[News] [Paper Feed] [Issues] [Authors] [Archives] [Contact]
PHRACK
.:: PHRACK NEWS ::.
Live and let die
posted by Phrack Staff
==Phrack Magazine==
C F P
P H R A C K 7 1
Dear readers, let's take a moment for poetry:

Capturar el trafico de una dirección ip

Ensamblar paquetes

Identificar un paquete y hacer el filtrado en este caso HTTP




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,
One equal temper of heroic hearts,
Made weak by time and fate, but strong in will
To strive, to seek, to find,
and not to yield [control].
PHRACK 71 awaits your input, the impatient accepted will be sent strai
ght to
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
possible outcomes:
1. The article is accepted, it can be published in the paper feed
if
you want. Congratz.
2. The article is accepted, but will be published in the final rel
ease.
If you decide to contribute to PWN or linenoise (lul), this wil
l be
the case. Nice one.
3. The article is not *yet* suitable for PHRACK but nonetheless wo
uld
be with additional work. A Phrack Staff reviewer is assigned to
help
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


altoromutual.com/index.jsp
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Sign In | Contact Us | Feedback | Search
AltoroMutual
DEMO SITE ONLY
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 with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.
Real Estate Financing
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
Business Credit Cards
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.
Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.
Privacy and Security
The 2000 employees of A
are dedicated to protectin
privacy and security. We p
provide you with the inform
resources that you need t
secure your information a
confidential. This is our pr
Win a Samsung Galaxy
smartphone
Completing this short surv
you in a draw for 1 of 5 Sa
Galaxy S10 smartphones!
forward to hearing your im
feedback.
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 featu
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting

AltoroMutual

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

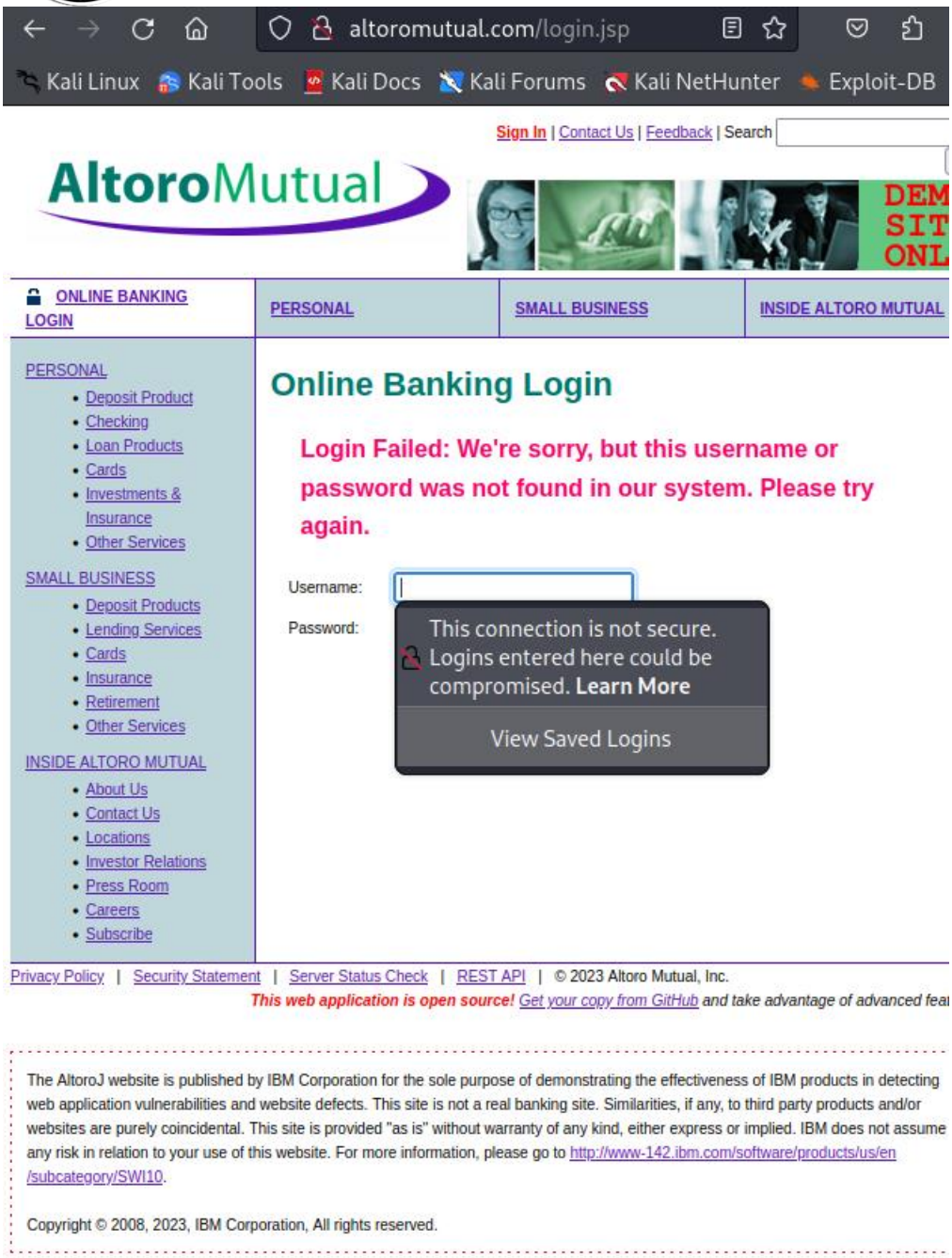
Online Banking Login

Username: fabian

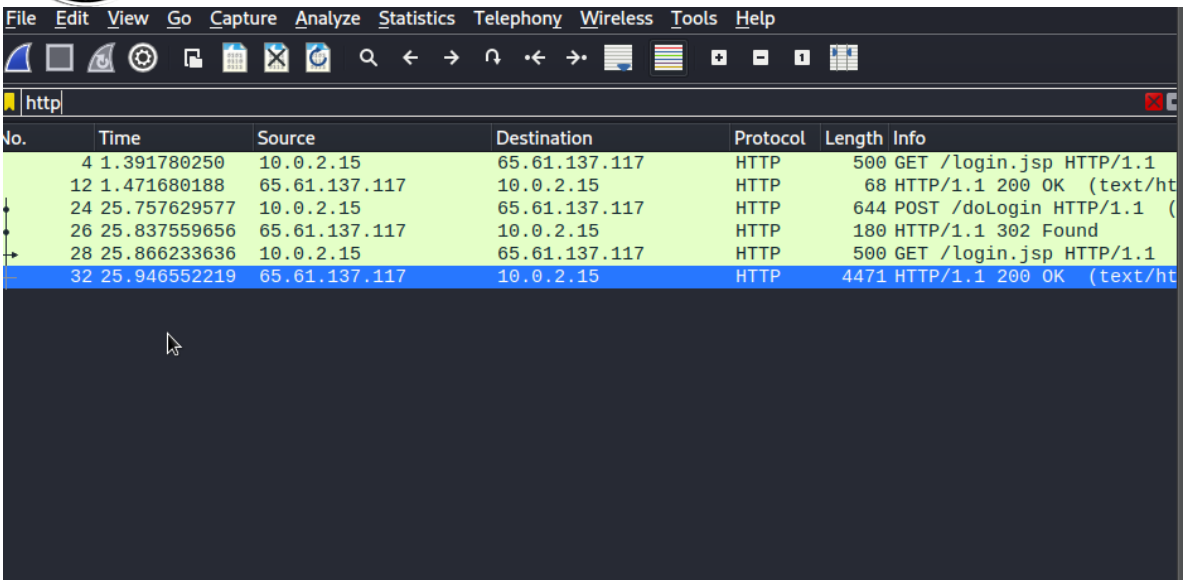
Password: ••••••••••

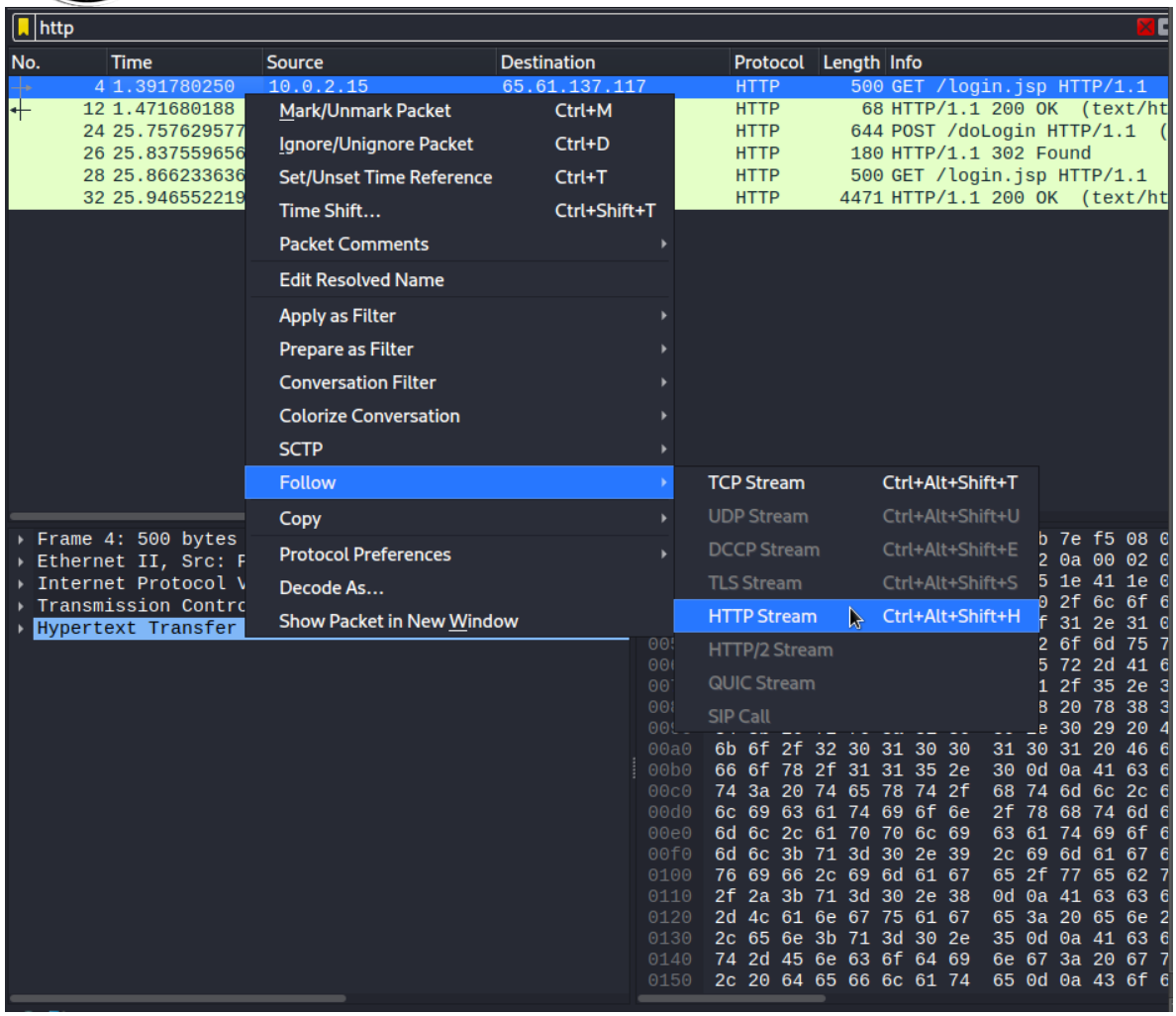
Login

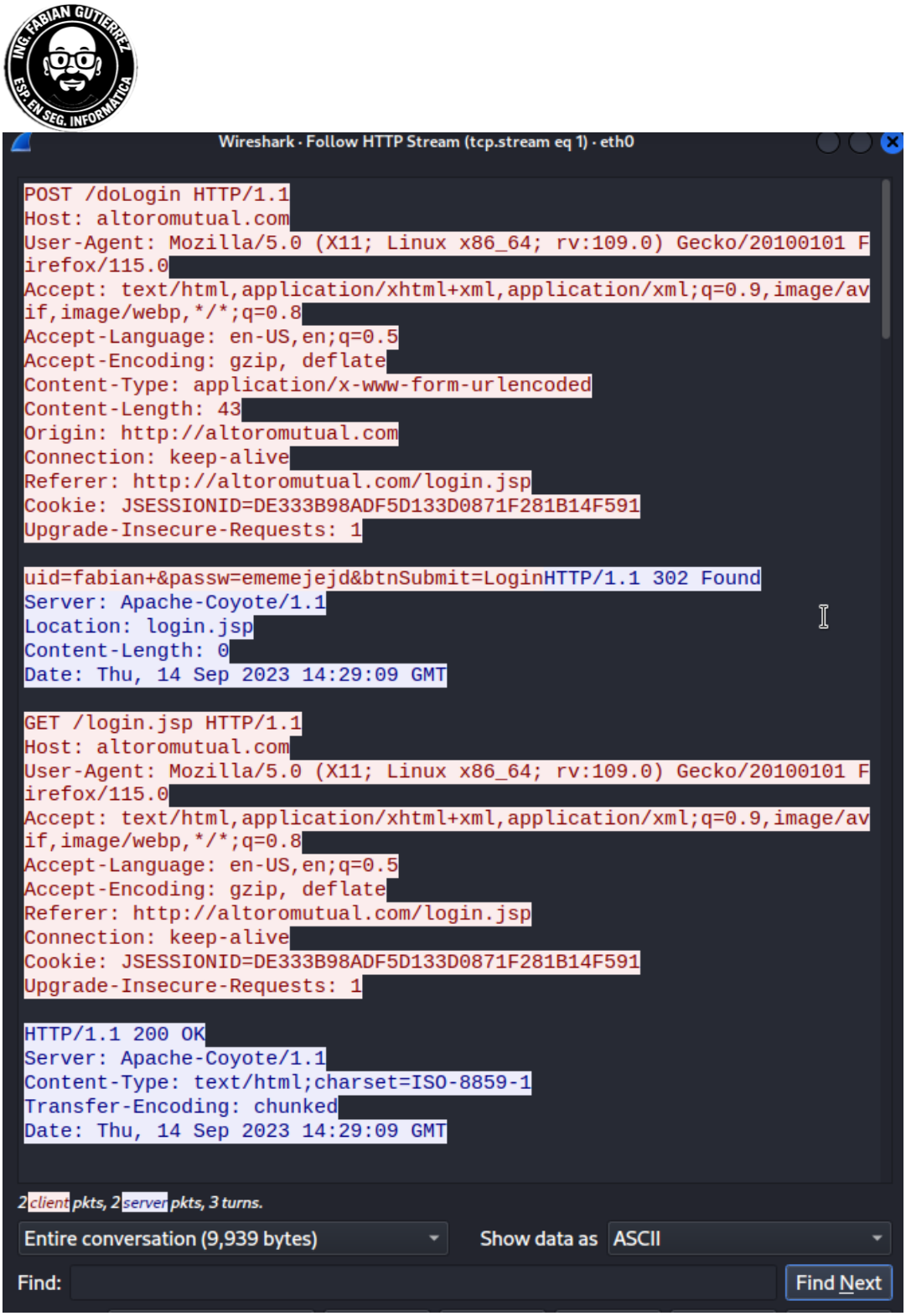
This web application is open source! Get your copy from GitHub and take advantage of advanced featu



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 HTTP 68 HTTP/1.1 200 OK (text/ht
24 25.757629577 HTTP 644 POST /doLogin HTTP/1.1 (
26 25.837559656 HTTP 180 HTTP/1.1 302 Found
28 25.866233636 HTTP 500 GET /login.jsp HTTP/1.1
32 25.946552219 HTTP 4471 HTTP/1.1 200 OK (text/ht
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
SIP Call
Frame 4: 500 bytes
Ethernet II, Src: P
Internet Protocol V
Transmission Contro
Hypertext Transfer
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 F
irefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,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 F
irefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,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

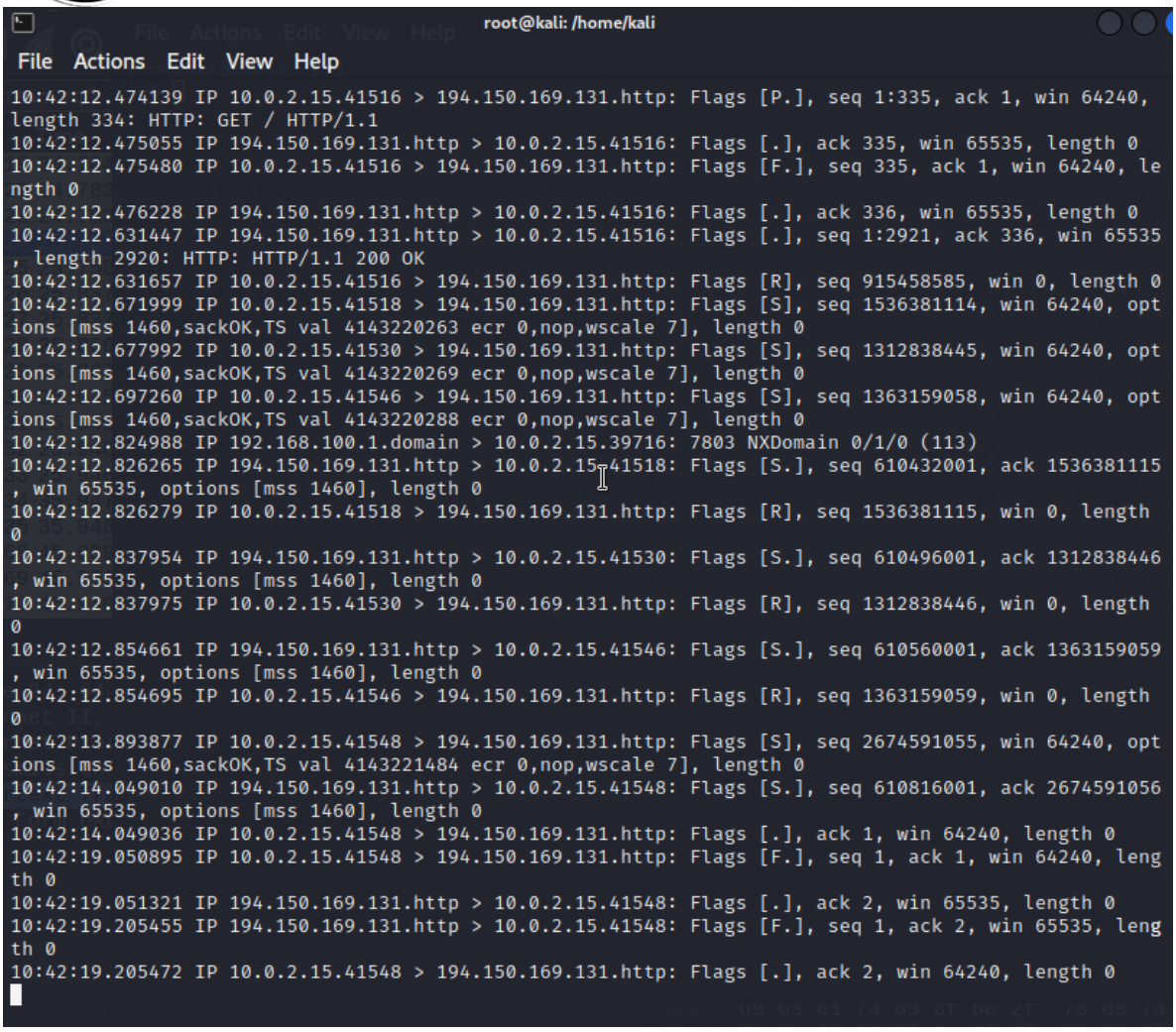
```
┌──(root㉿kali)-[/home/kali]
└─# tcpdump -h
tcpdump version 4.99.4
libpcap version 1.10.4 (with TPACKET_V3)
OpenSSL 3.0.10 1 Aug 2023
Usage: tcpdump [-AbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ] [--count]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -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)-[/home/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)-[/home/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
```

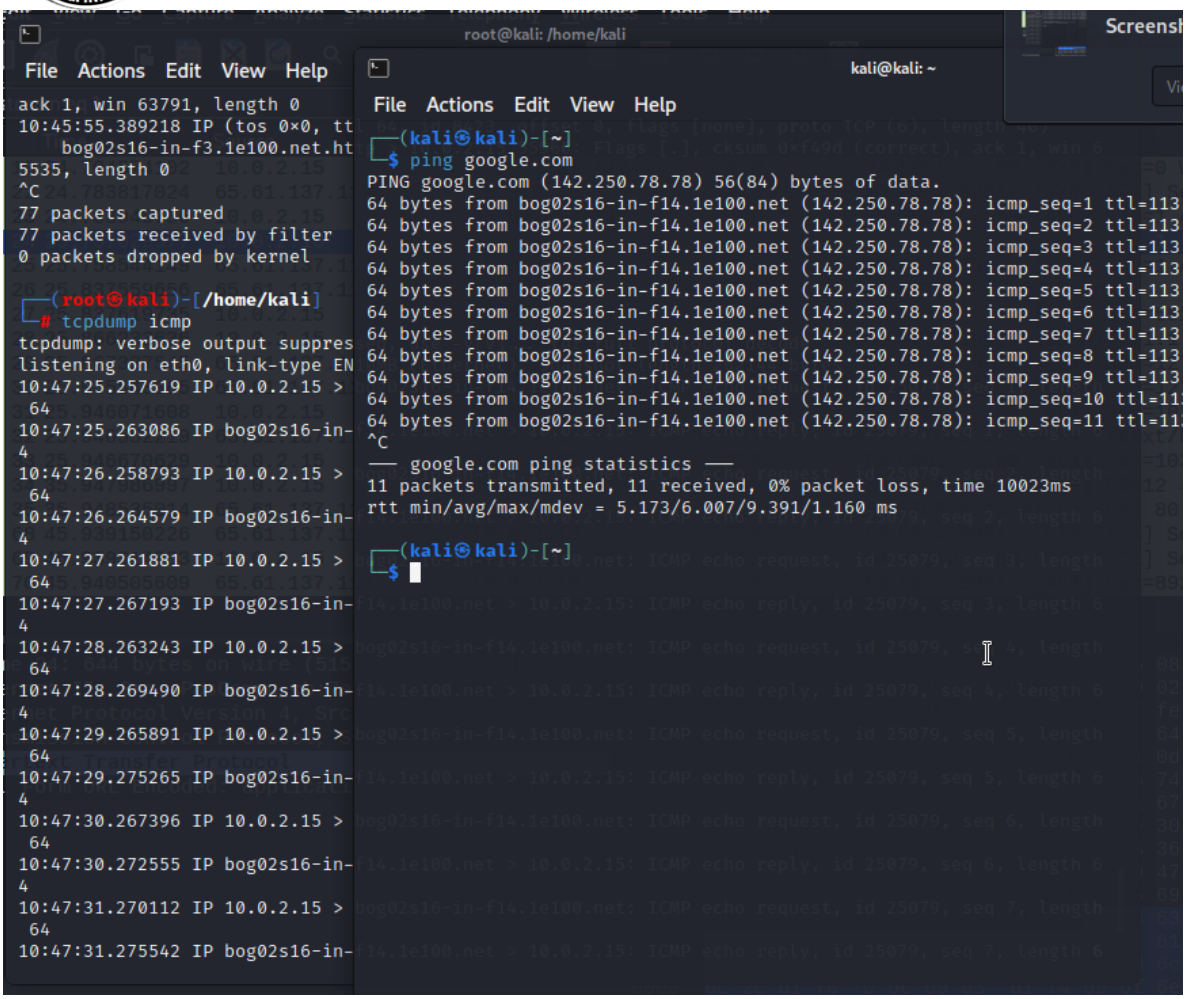


tcpdump -v – i eth0

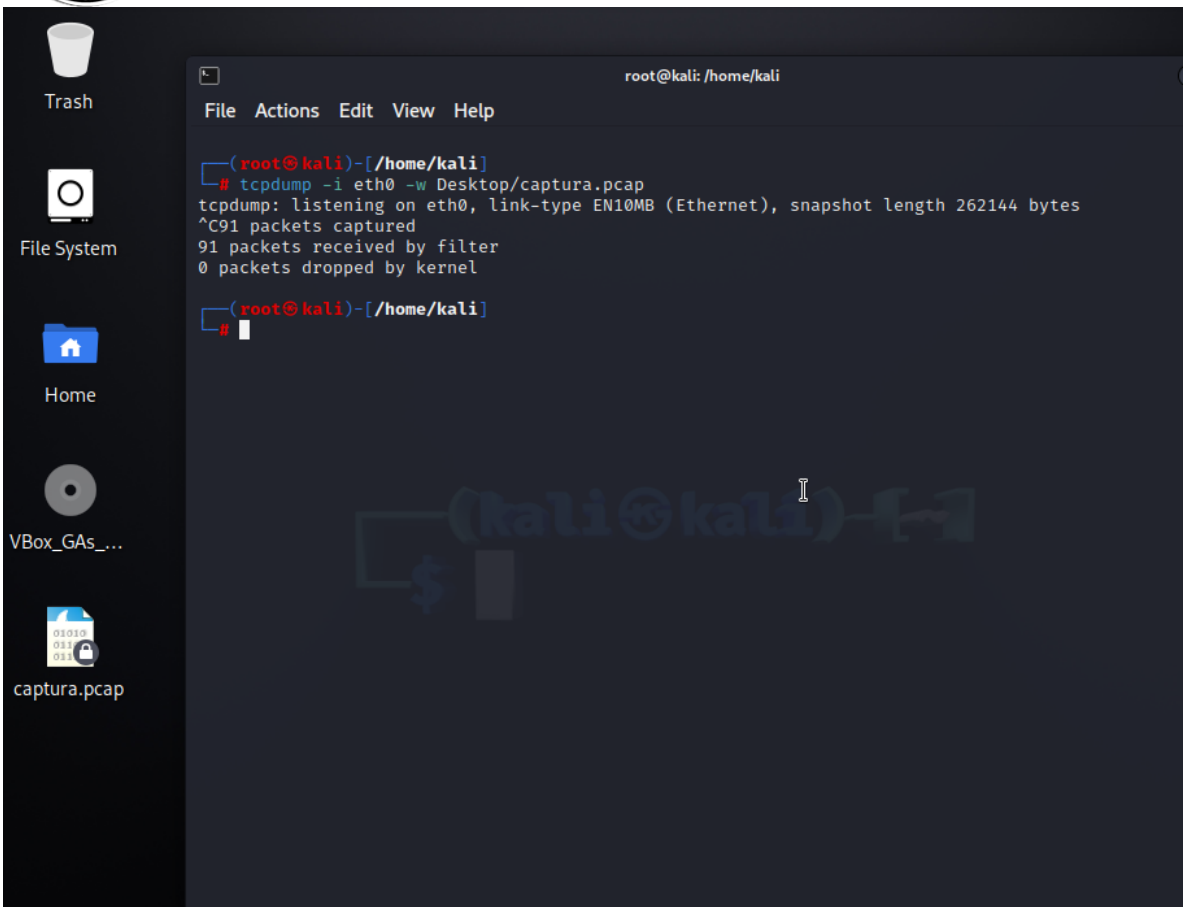
```
┌──(root㉿kali)-[/home/kali]
└─# tcpdump -v -i eth0
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:45:24.700739 IP (tos 0×0, ttl 64, id 29032, offset 0, flags [DF], proto TCP (6), length 40)
    10.0.2.15.55960 > bog02s16-in-f3.1e100.net.http: Flags [.], cksum 0×e966 (incorrect → 0×fb6e),
ack 633984703, win 63791, length 0
10:45:24.701391 IP (tos 0×0, 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 0×f49d (correct), ack 1, win 6
5535, length 0
10:45:24.765091 IP (tos 0×0, 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 0×0, 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 0×0, 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 0×0, 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)
```

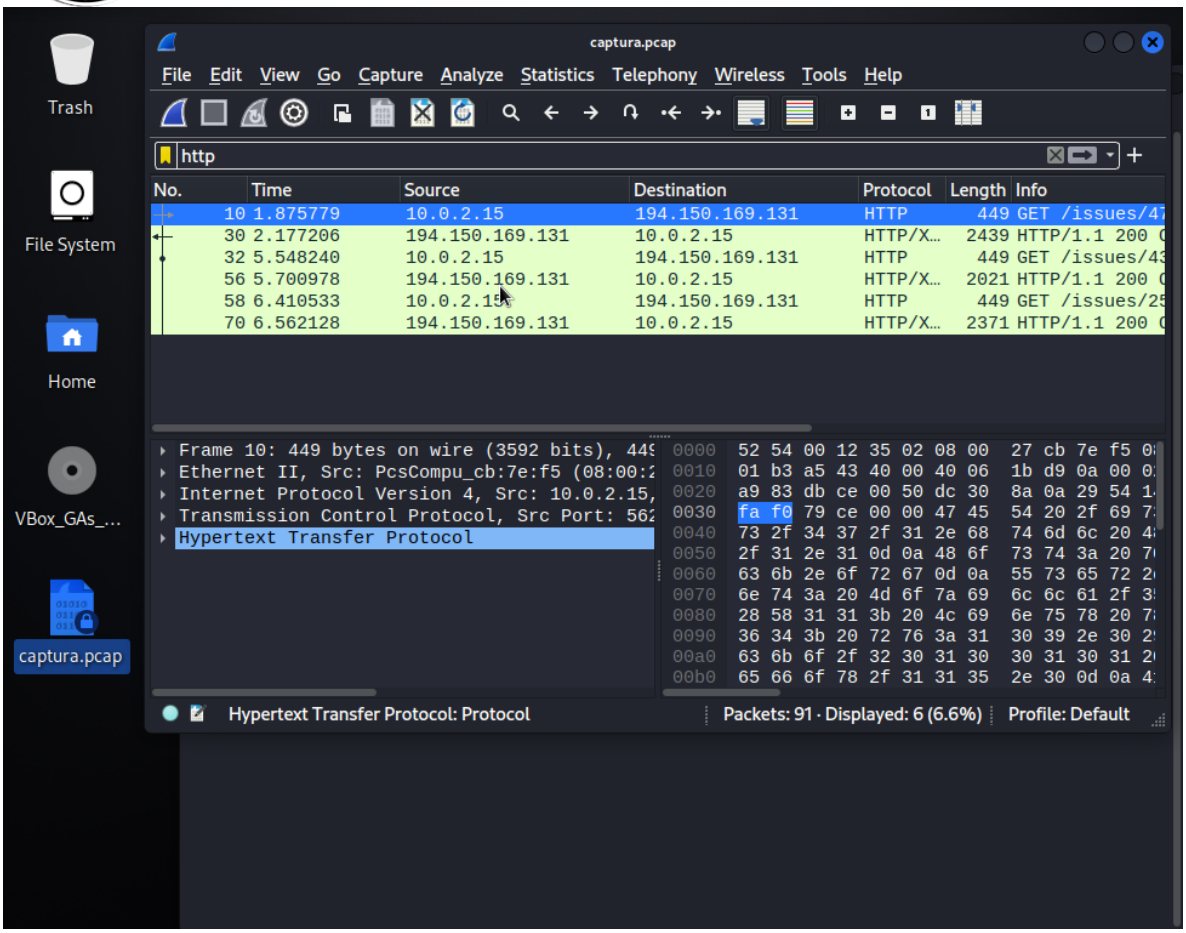
tcpdump icmp

```
┌──(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
```



tcpdump -i eth0 -w Desktop/captura.pcap


Trash
File System
Home
VBox_GAs_...
captura.pcap
root@kali: /home/kali
File Actions Edit View Help
┌──(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]
└─#



Tcpdump -r captura.pcap


```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# 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, opt
ions [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 65
5233155:655233179, 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 6553
5, 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 65
535, 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)-[/home/kali/Desktop]
└─# 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)
```