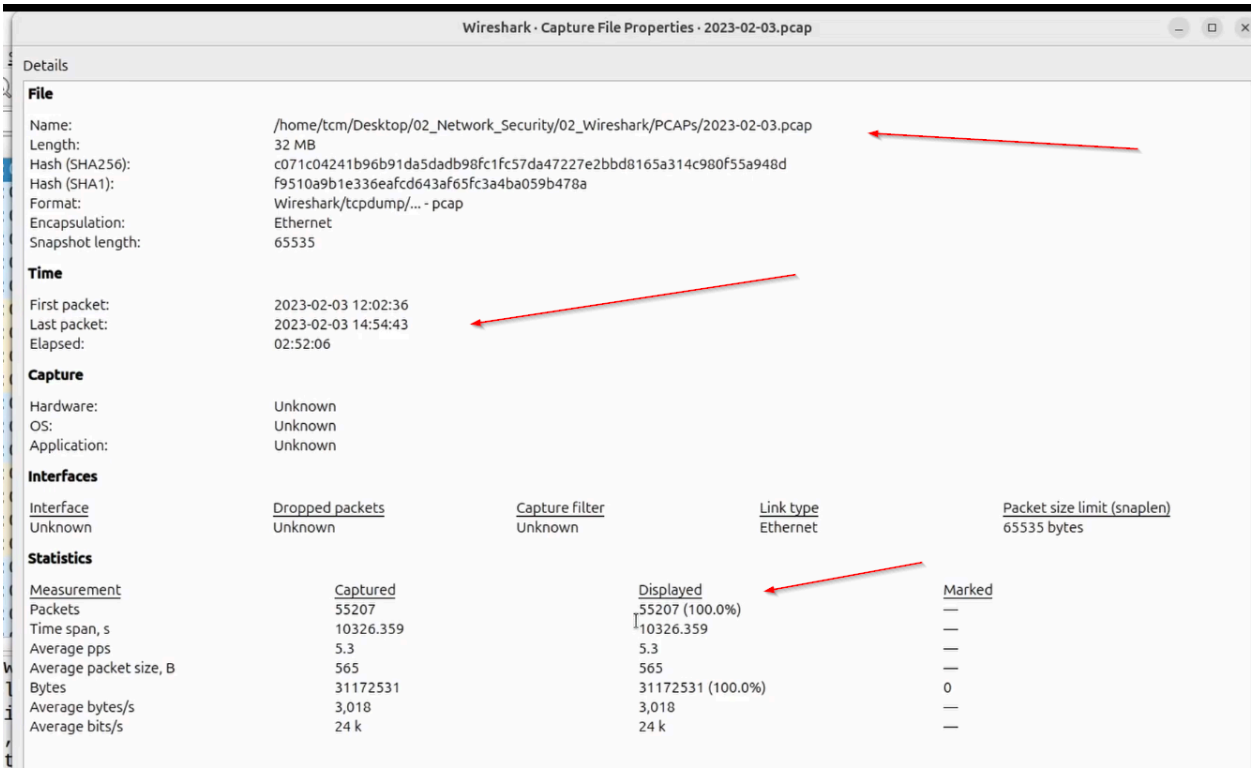
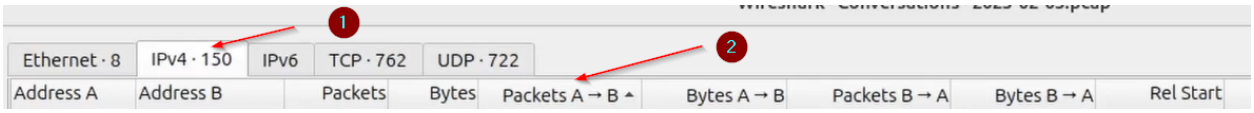
Methodology

1.) See file summary



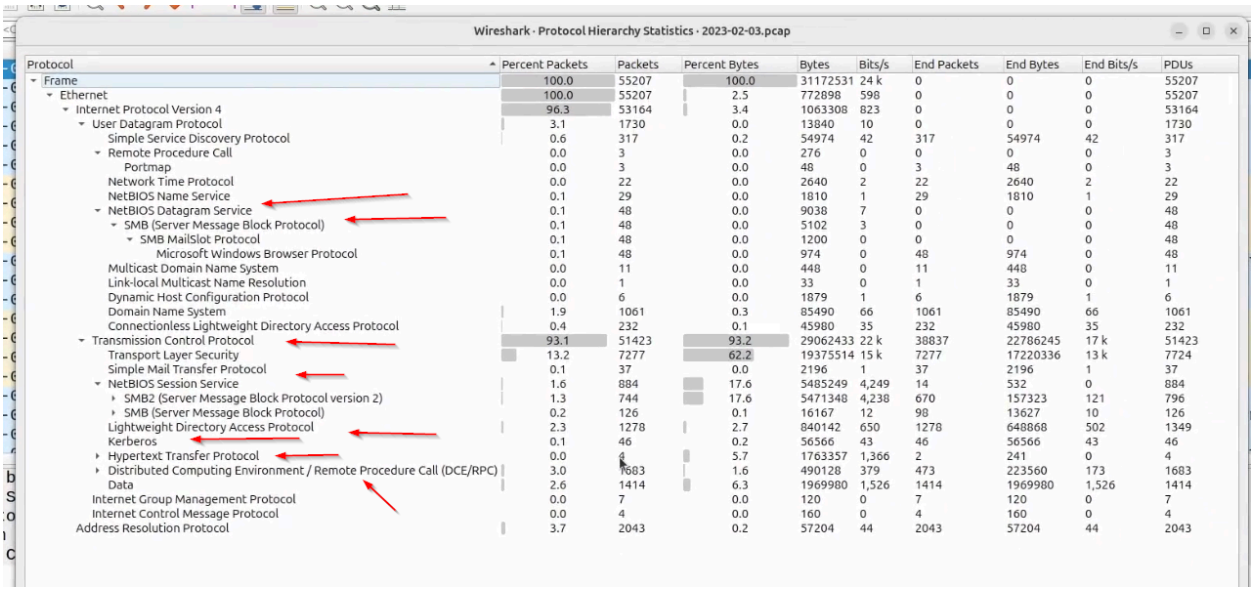
2.) Conversation

⇒ Most IP talk to another IPs and double click packet option

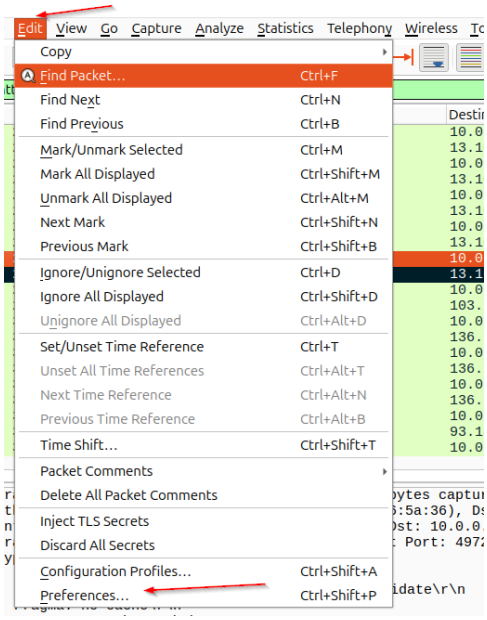


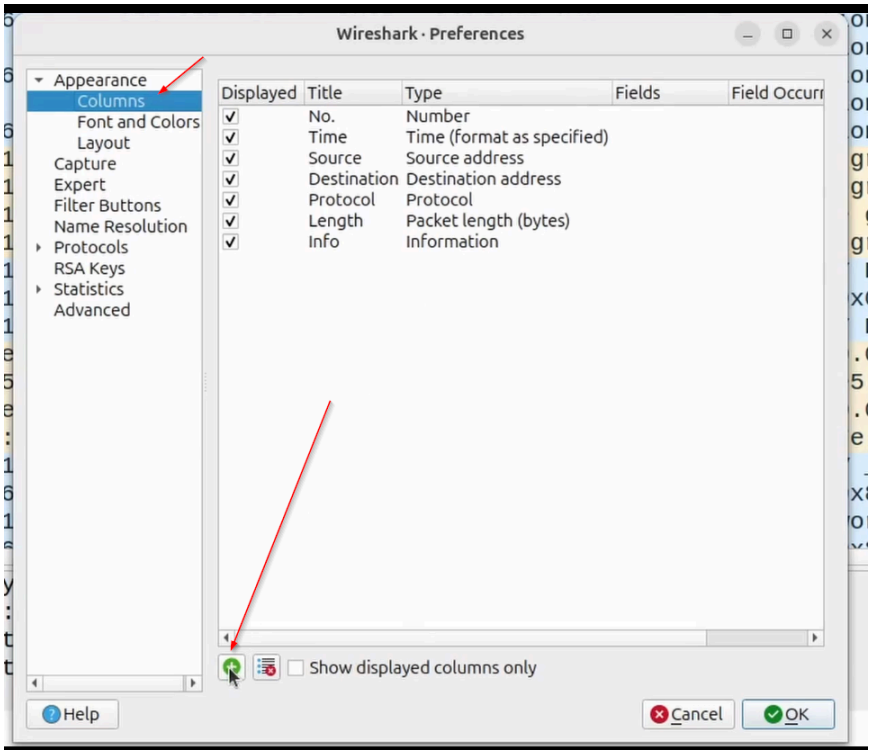
3.) Protocol Hierarchy

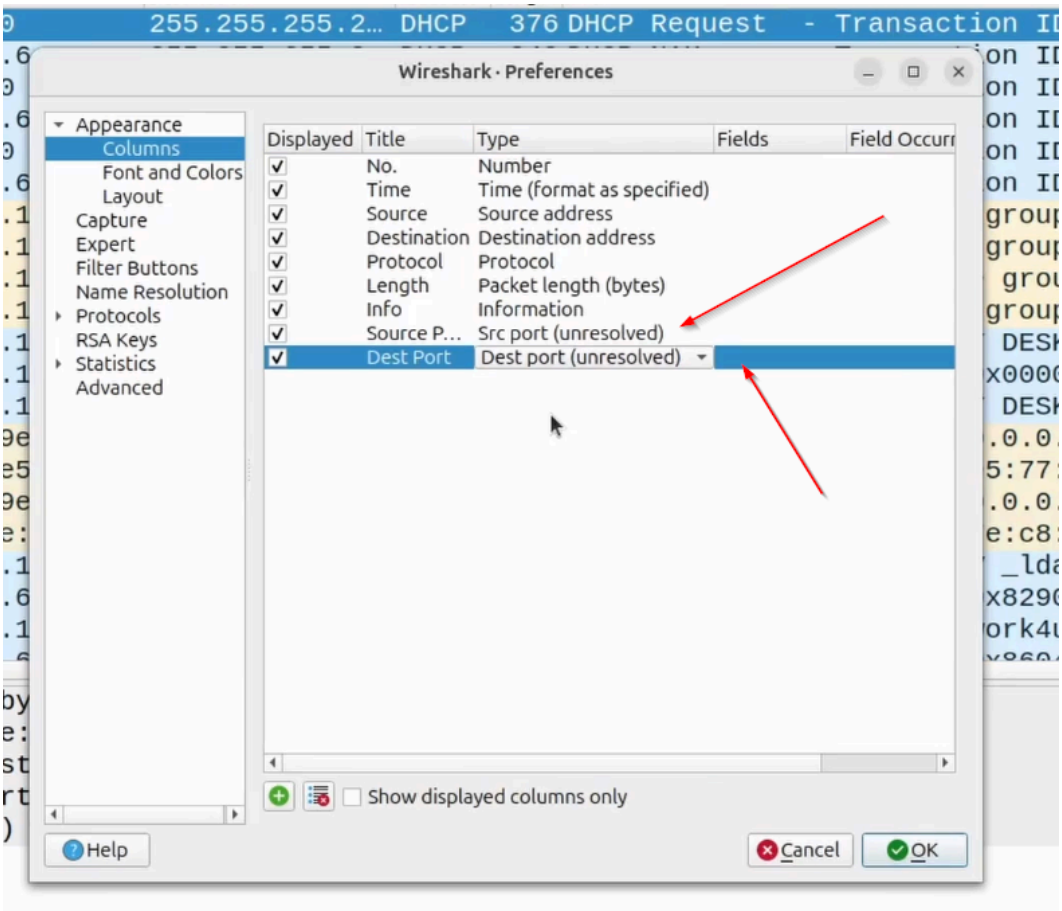
⇒ Most Port communication case and some suspicious port find

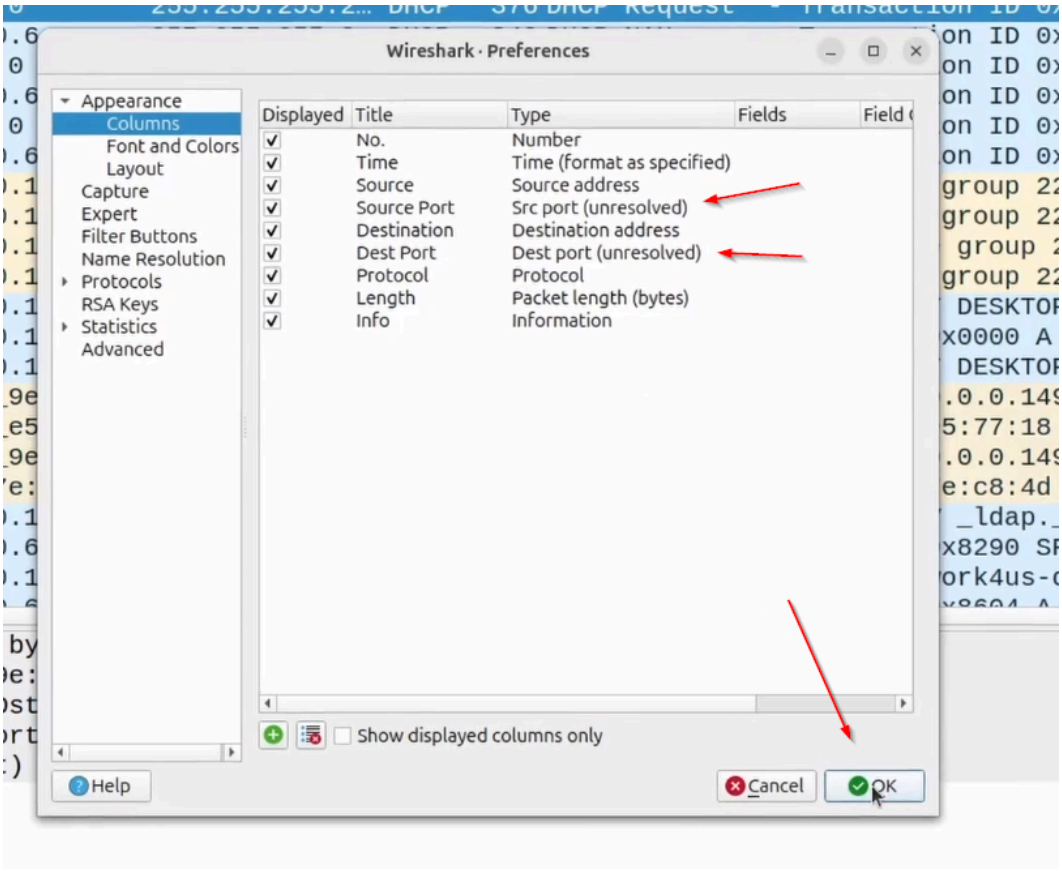


4.) Add two columns (source port , destination port)


Edit View Go Capture Analyze Statistics Telephony Wireless
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Selected Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Selected Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comments
Delete All Packet Comments
Inject TLS Secrets
Discard All Secrets
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P

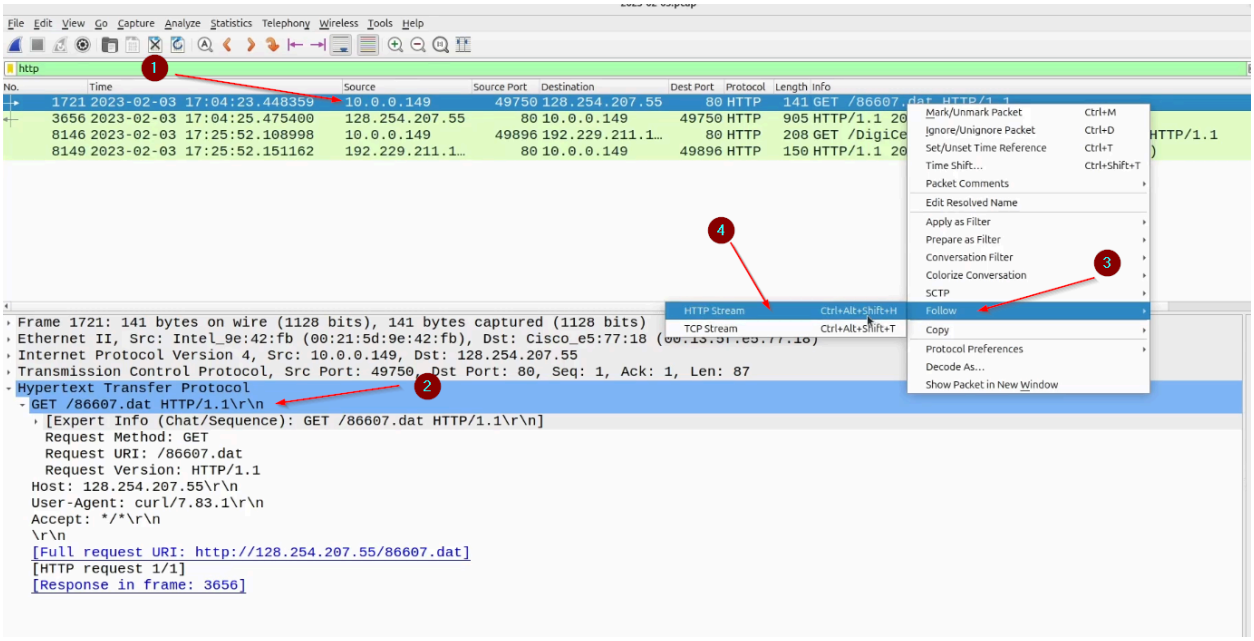

Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
Displayed Title Type Fields Field Occurr
No. Number
Time Time (format as specified)
Source Source address
Destination Destination address
Protocol Protocol
Length Packet length (bytes)
Info Information
Show displayed columns only
Help
Cancel
OK


255.255.255.2… DHCP 376 DHCP Request - Transaction ID
Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
Displayed
Title
Type
Fields
Field Occurr
No. Number
Time Time (format as specified)
Source Source address
Destination Destination address
Protocol Protocol
Length Packet length (bytes)
Info Information
Source P… Src port (unresolved)
Dest Port Dest port (unresolved)
Show displayed columns only
Help
Cancel
OK



5.) Filter to HTTP port

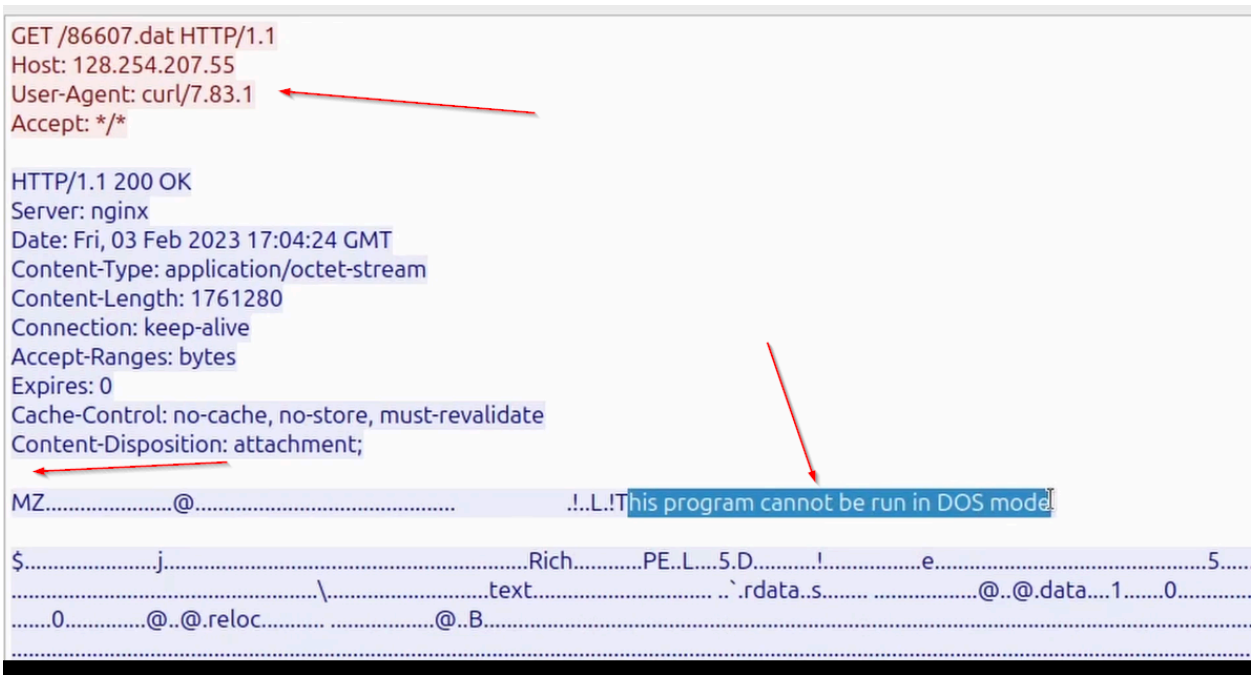
⇒ We before find four http packet so i analysis



IOC:

user agent

MZ file signature refer google (list of file signatures)

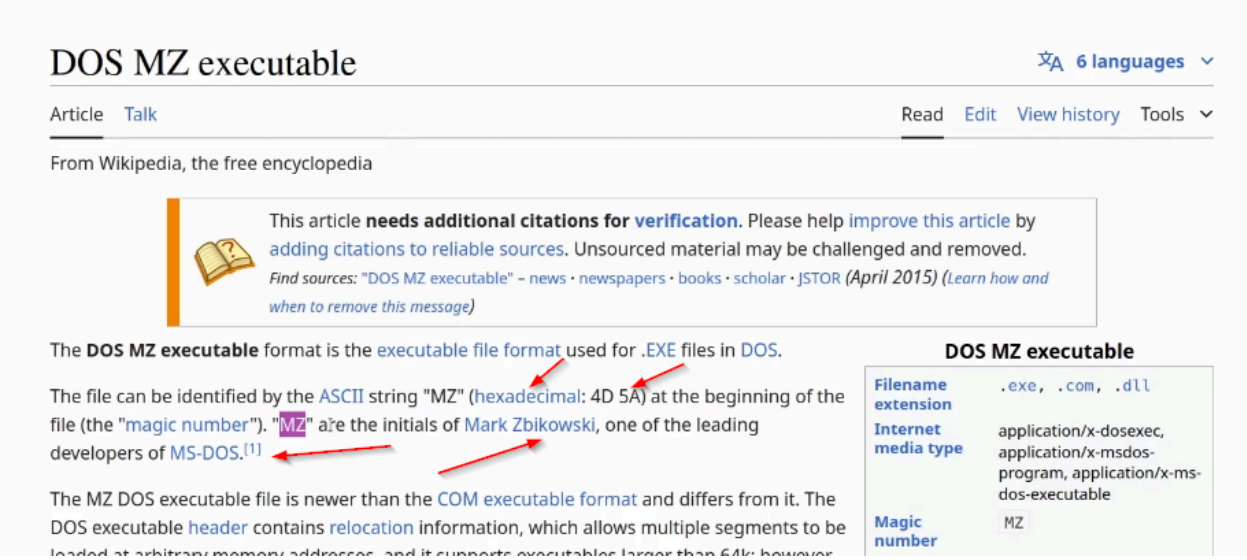


ex

52 4E 43 01 52 4E 43 02	RNC␖ RNC␖	0		Compressed file using Rob Northen Compression (version 1 and 2) algorithm[13]
4E 55 52 55 49 4D 47 4E 55 52 55 50 41 4C	NURUIMG NURUPAL	0	nui nup	nuru ASCII/ANSI image and palette files[14]
53 44 50 58 (big-endian format)	SDPX	0	dpx	SMPTE DPX image
58 50 44 53 (little-endian format)	XPDS			
76 2F 31 01	v/1␖	0	exr	OpenEXR image
42 50 47 FB	BPGû	0	bpg	Better Portable Graphics format[15]
FF D8 FF DB	ÿØÿÛ	0	jpg jpeg	JPEG raw or in the JFIF or Exif file format[16]
FF D8 FF E0 00 10 4A 46 49 46 00 01	ÿØÿà␖␖JFIF␖␖			
FF D8 FF EE	ÿØÿî			
FF D8 FF E1 ?? ?? 45 78 69 66 00 00	ÿØÿá??Exif␖␖			
FF D8 FF E0	ÿØÿà	0	jpg	JPEG raw or in the JFIF or Exif file format[16]
			jp2	

or

30 37 30 37 30 37	070707	0	cpio	cpio archive file[20]
4D 5A	MZ	0	exe dll mui sys scr cpl ocx ax iec ime rs tsp fon efi	DOS MZ executable and its descendants (including NE and PE)



DOS MZ executable

6 languages

Article Talk | Read Edit View history Tools

From Wikipedia, the free encyclopedia

This article **needs additional citations for verification**. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed.
Find sources: "DOS MZ executable" – news · newspapers · books · scholar · JSTOR *(April 2015)* *(Learn how and when to remove this message)*

The **DOS MZ executable** format is the executable file format used for .EXE files in DOS.

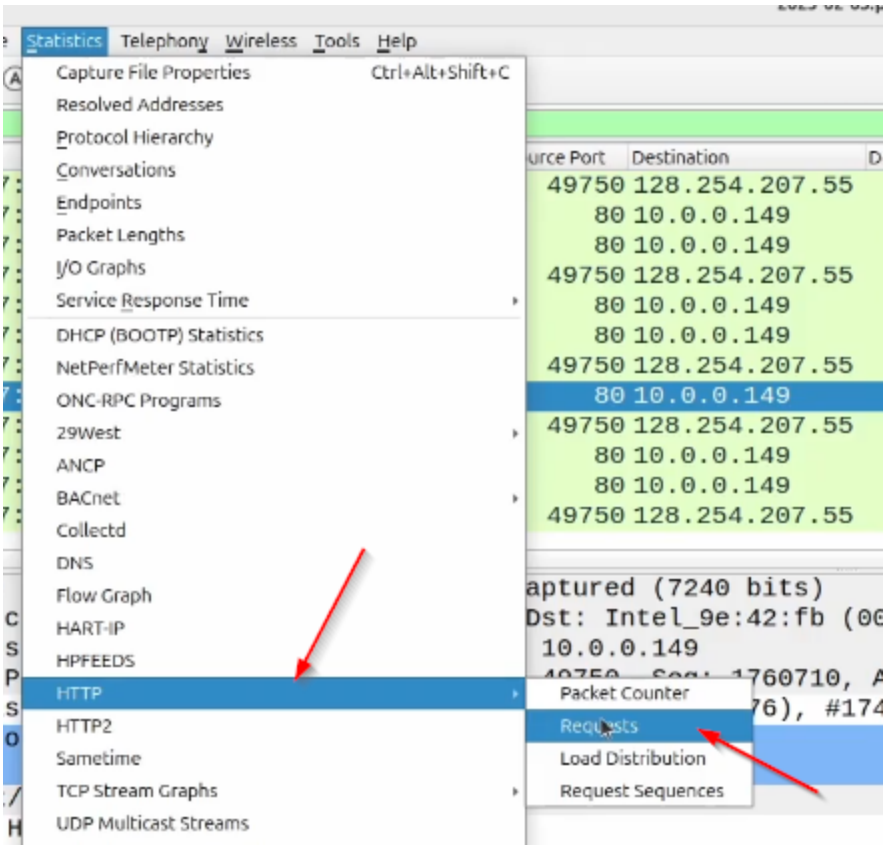
The file can be identified by the ASCII string "MZ" (hexadecimal: 4D 5A) at the beginning of the file (the "magic number"). "MZ" are the initials of Mark Zbikowski, one of the leading developers of MS-DOS.[1]

The MZ DOS executable file is newer than the COM executable format and differs from it. The DOS executable header contains relocation information, which allows multiple segments to be

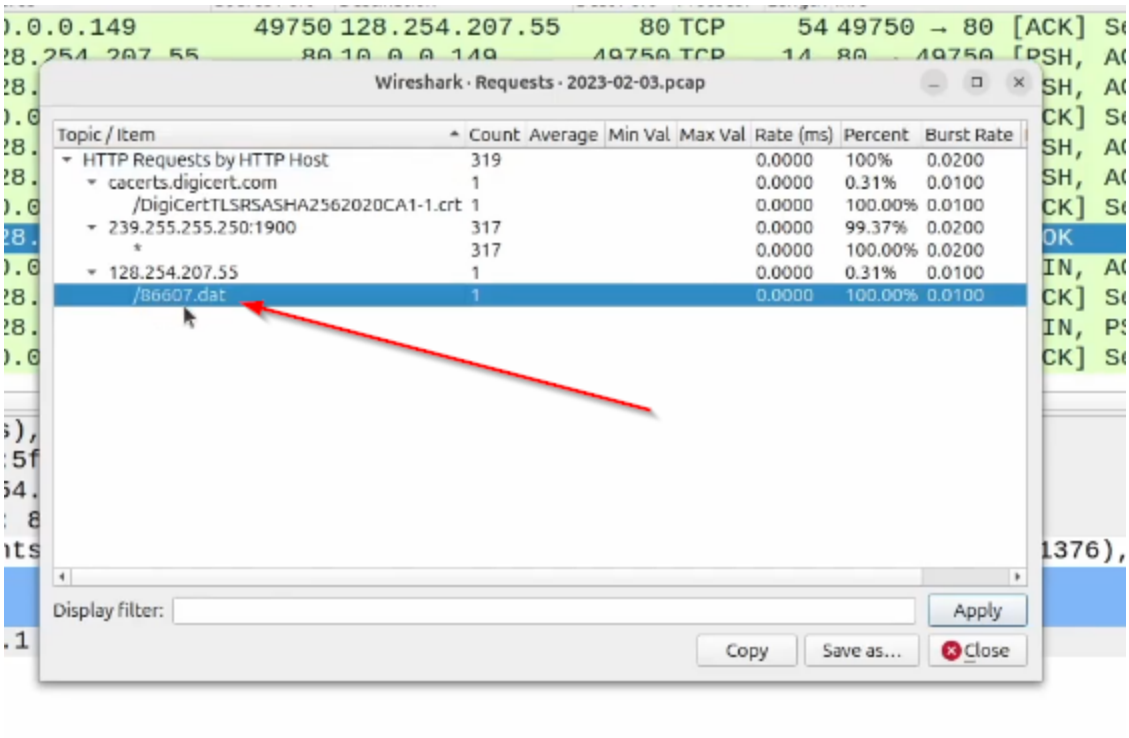
DOS MZ executable

Filename extension	.exe, .com, .dll
Internet media type	application/x-dosexec, application/x-msdos-program, application/x-ms-dos-executable
Magic number	MZ

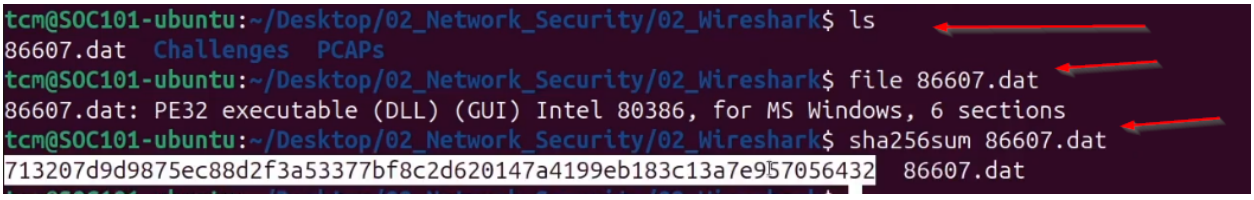
6.) HTTP Request to find files



Immediately found files

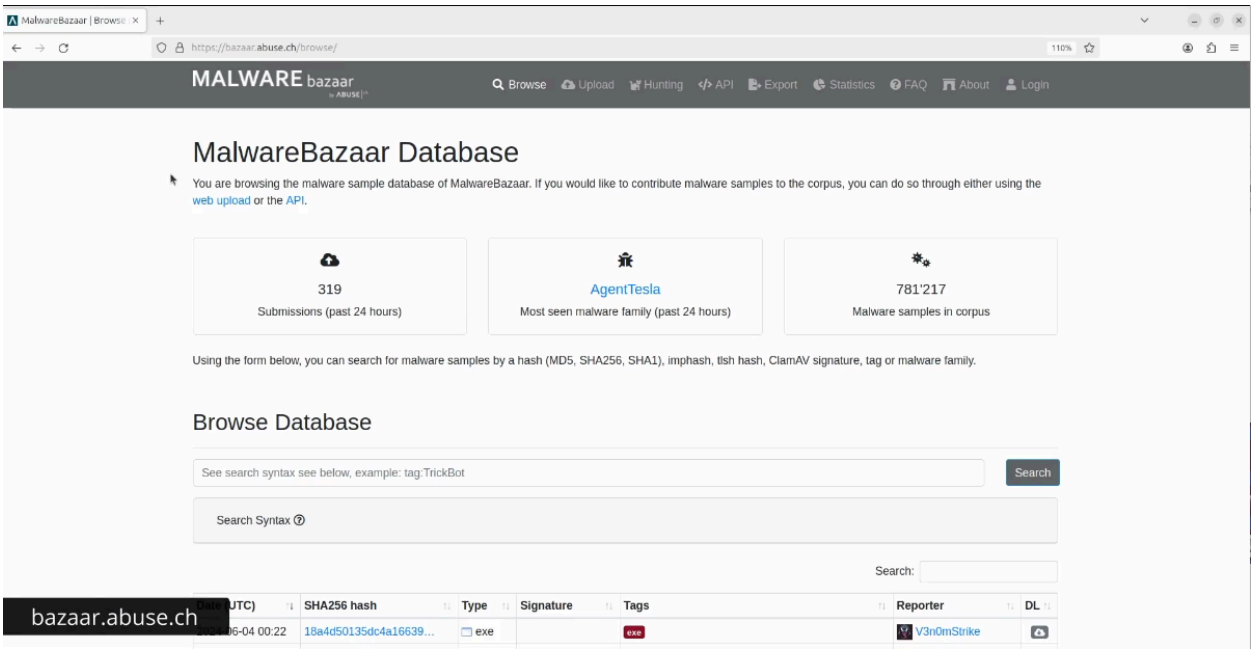


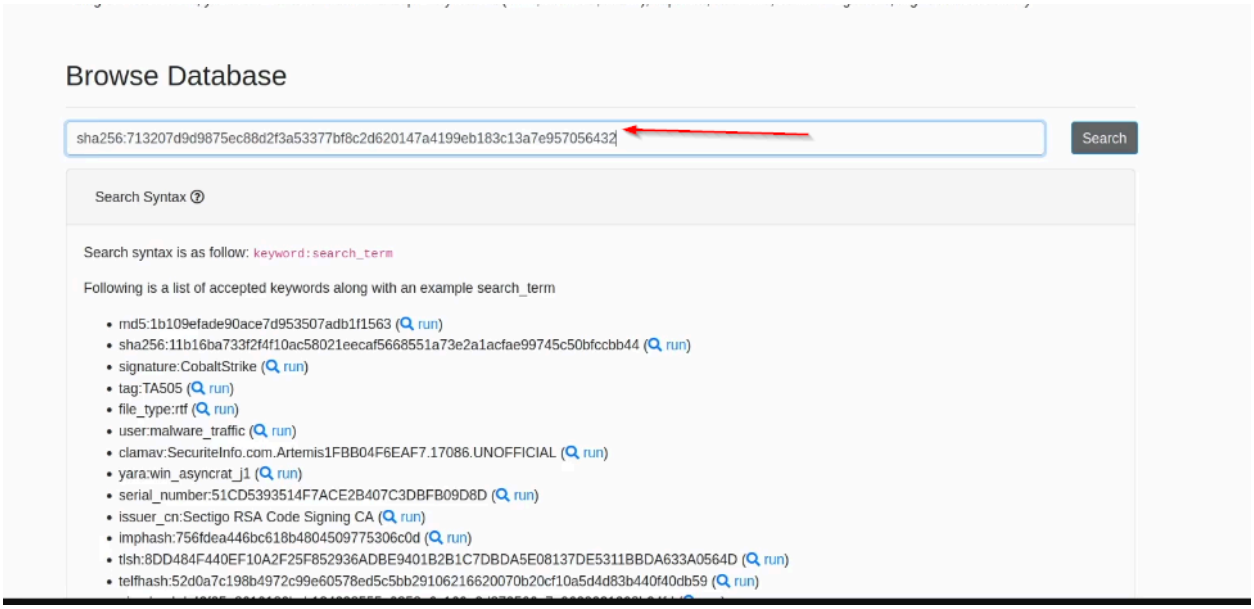
Next export file use **wireshark export objective** features and check file repetition



virus total

malware bazaar

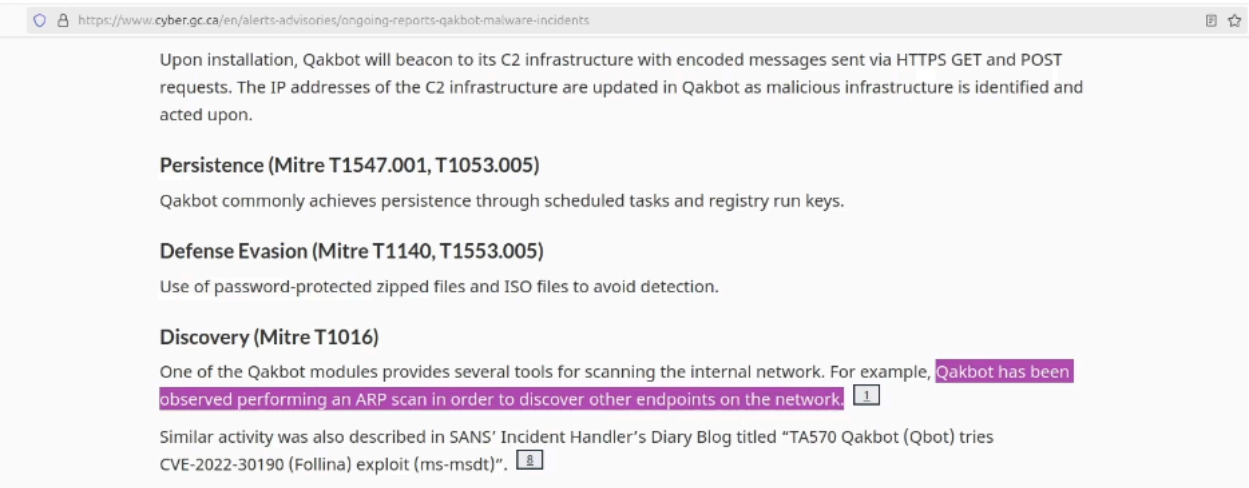

MalwareBazaar | Browse
https://bazaar.abuse.ch/browse/
MALWARE bazaar
Browse
Upload
Hunting
API
Export
Statistics
FAQ
About
Login
MalwareBazaar Database
You are browsing the malware sample database of MalwareBazaar. If you would like to contribute malware samples to the corpus, you can do so through either using the web upload or the API.
319
Submissions (past 24 hours)
AgentTesla
Most seen malware family (past 24 hours)
781'217
Malware samples in corpus
Using the form below, you can search for malware samples by a hash (MD5, SHA256, SHA1), imphash, tlsh hash, ClamAV signature, tag or malware family.
Browse Database
See search syntax see below, example: tag:TrickBot
Search
Search Syntax
Search:
bazaar.abuse.ch
SHA256 hash
Type
Signature
Tags
Reporter
DL
18a4d50135dc4a16639...
exe
V3n0mStrike


Browse Database
sha256:713207d9d9875ec88d2f3a53377bf8c2d620147a4199eb183c13a7e957056432
Search
Search Syntax
Search syntax is as follow: keyword:search_term
Following is a list of accepted keywords along with an example search_term
md5:1b109efade90ace7d953507adb1f1563 (run)
sha256:11b16ba733f2f4f10ac58021eecaf5668551a73e2a1acfae99745c50bfccbb44 (run)
signature:CobaltStrike (run)
tag:TA505 (run)
file_type:rtf (run)
user:malware_traffic (run)
clamav:SecuriteInfo.com.Artemis1FBB04F6EAF7.17086.UNOFFICIAL (run)
yara:win_asyncrat_j1 (run)
serial_number:51CD5393514F7ACE2B407C3DBFB09D8D (run)
issuer_cn:Sectigo RSA Code Signing CA (run)
imphash:756fdea446bc618b4804509775306c0d (run)
tlsh:8DD484F440EF10A2F25F852936ADBE9401B2B1C7DBDA5E08137DE5311BBDA633A0564D (run)
telfhash:52d0a7c198b4972c99e60578ed5c5bb29106216620070b20cf10a5d4d83b440f40db59 (run)

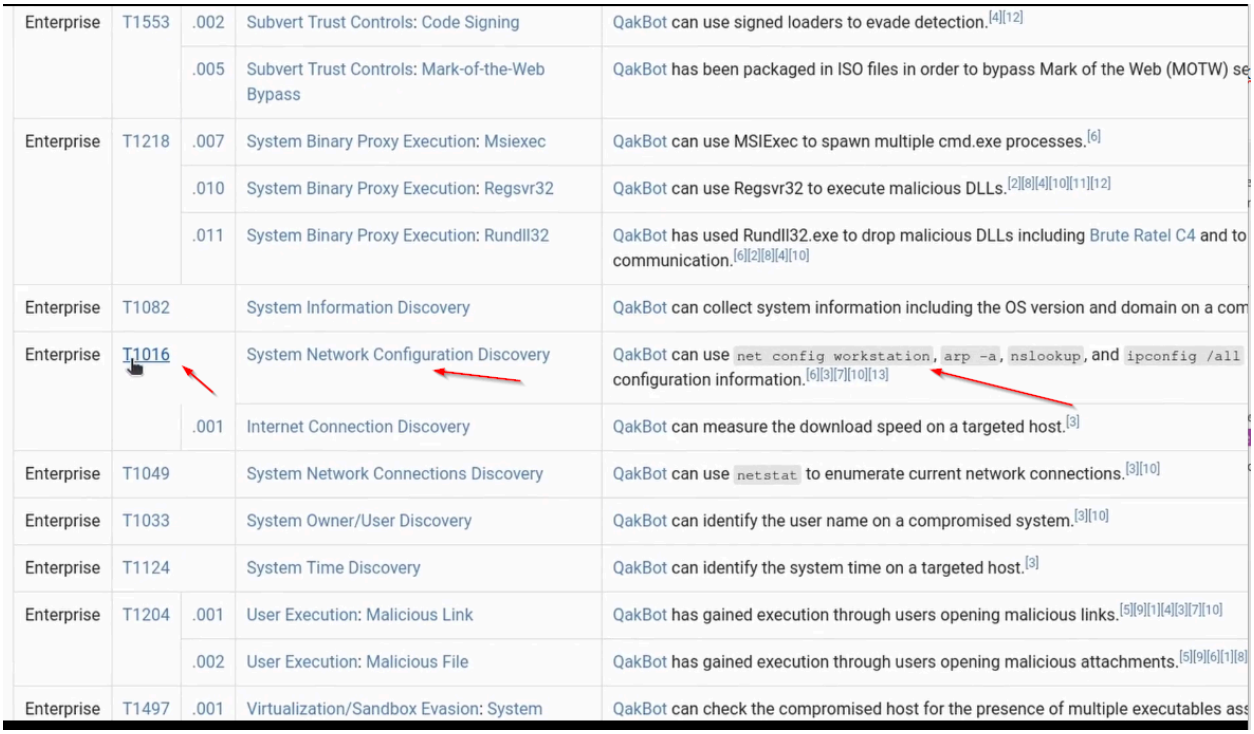
Result:

Perform malware research and what does that malware after install?

⇒ Next we do refer internet and (search what does Quakbot OR Quakbot IOC)



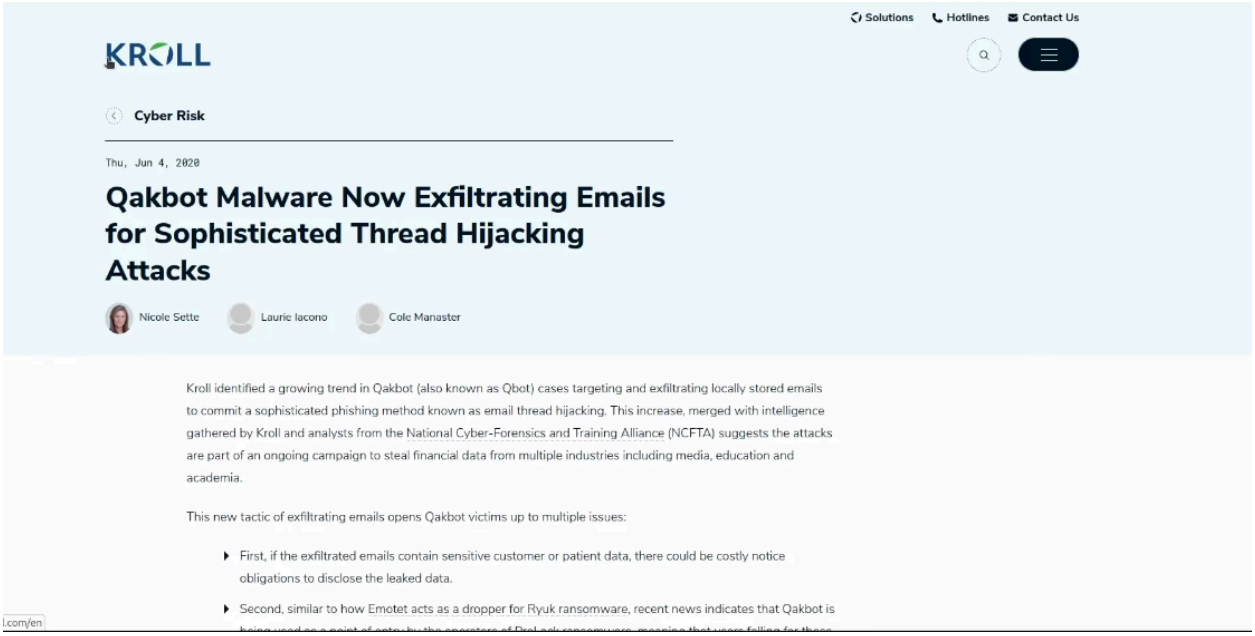
Mitre frame to malware post work anlaysis



Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	QakBot can use signed loaders to evade detection.[4][12]
		.005	Subvert Trust Controls: Mark-of-the-Web Bypass	QakBot has been packaged in ISO files in order to bypass Mark of the Web (MOTW) se
Enterprise	T1218	.007	System Binary Proxy Execution: Msiexec	QakBot can use MSIExec to spawn multiple cmd.exe processes.[6]
		.010	System Binary Proxy Execution: Regsvr32	QakBot can use Regsvr32 to execute malicious DLLs.[2][8][4][10][11][12]
		.011	System Binary Proxy Execution: Rundll32	QakBot has used Rundll32.exe to drop malicious DLLs including Brute Ratel C4 and to communication.[6][2][8][4][10]
Enterprise	T1082		System Information Discovery	QakBot can collect system information including the OS version and domain on a com
Enterprise	T1016		System Network Configuration Discovery	QakBot can use `net config workstation`, `arp -a`, `nslookup`, and `ipconfig /all` configuration information.[6][3][7][10][13]
		.001	Internet Connection Discovery	QakBot can measure the download speed on a targeted host.[3]
Enterprise	T1049		System Network Connections Discovery	QakBot can use `netstat` to enumerate current network connections.[3][10]
Enterprise	T1033		System Owner/User Discovery	QakBot can identify the user name on a compromised system.[3][10]
Enterprise	T1124		System Time Discovery	QakBot can identify the system time on a targeted host.[3]
Enterprise	T1204	.001	User Execution: Malicious Link	QakBot has gained execution through users opening malicious links.[5][9][1][4][3][7][10]
		.002	User Execution: Malicious File	QakBot has gained execution through users opening malicious attachments.[5][9][6][1][8]
Enterprise	T1497	.001	Virtualization/Sandbox Evasion: System	QakBot can check the compromised host for the presence of multiple executables ass

More articles

⇒ **Stealing emails** (exfiltrating them) from infected machines



7.) ARP traffic find

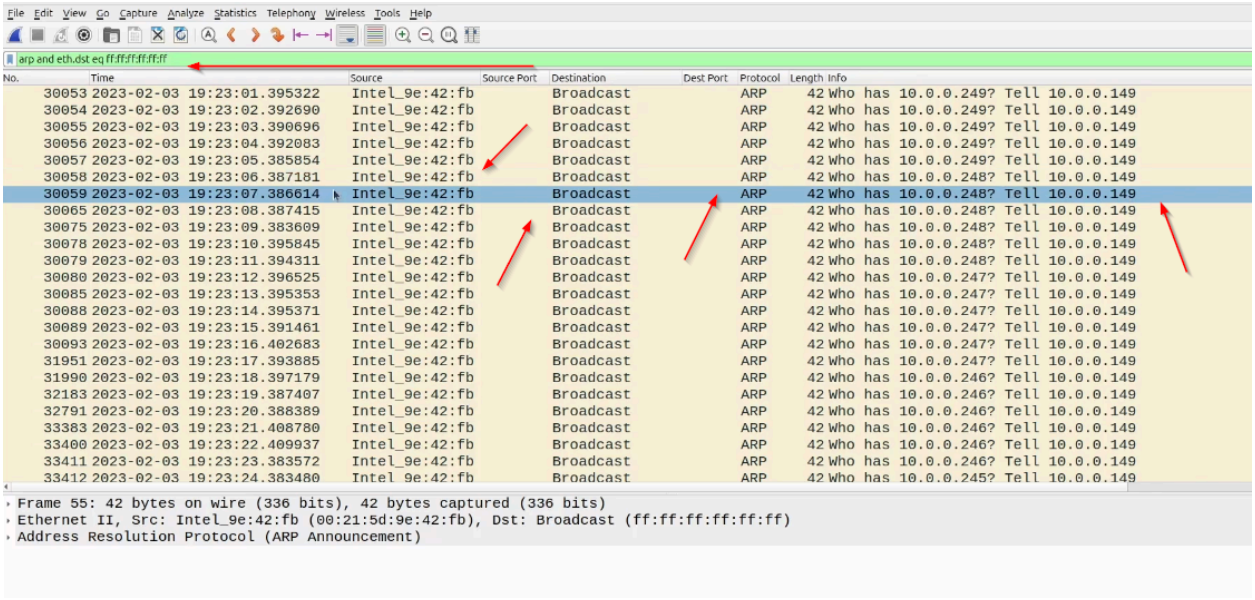
⇒ Malware **often uses** `arp` **(Address Resolution Protocol)** for **reconnaissance and lateral movement** inside a local network.

arp and eth.dst eq ff:ff:ff:ff:ff:ff

or

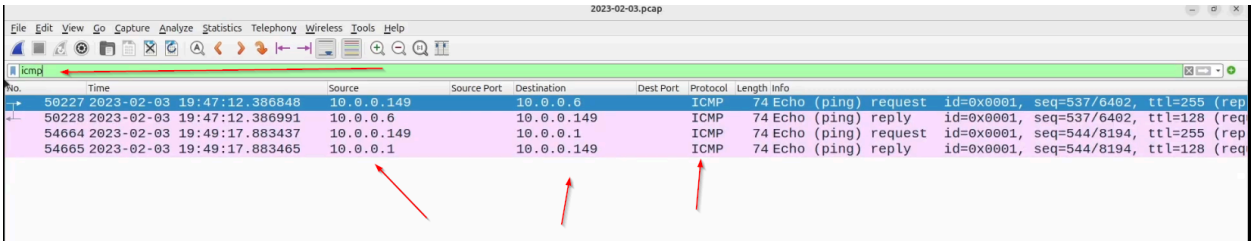
arp && eth.dst == ff:ff:ff:ff:ff:ff

⇒ See IP descending order to discovery that mean this perform recon



8.) Ping mean check live

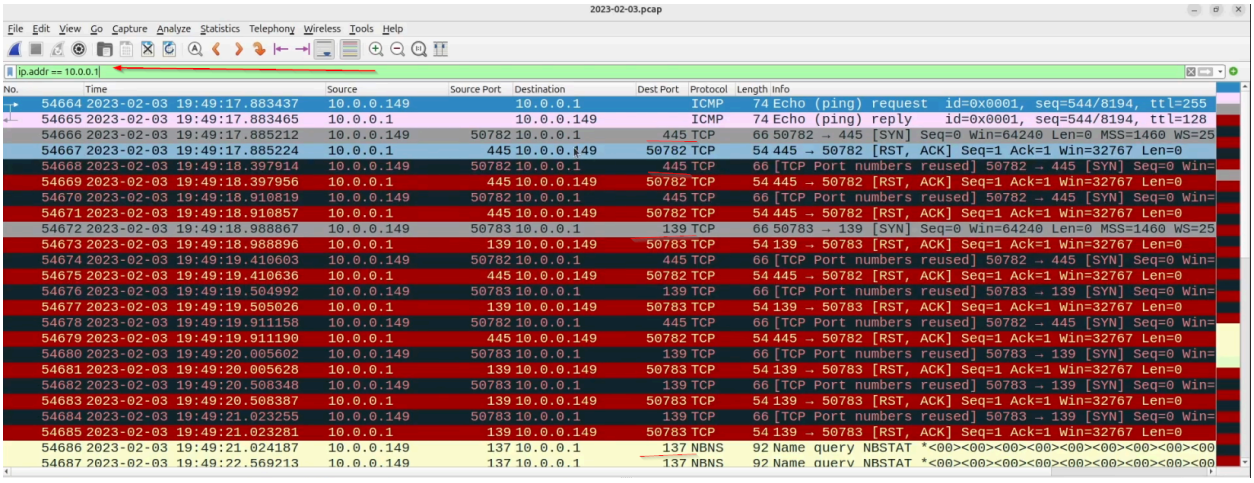
⇒ If ARP traffic come case we check ping (ICMP) traffic check come or not



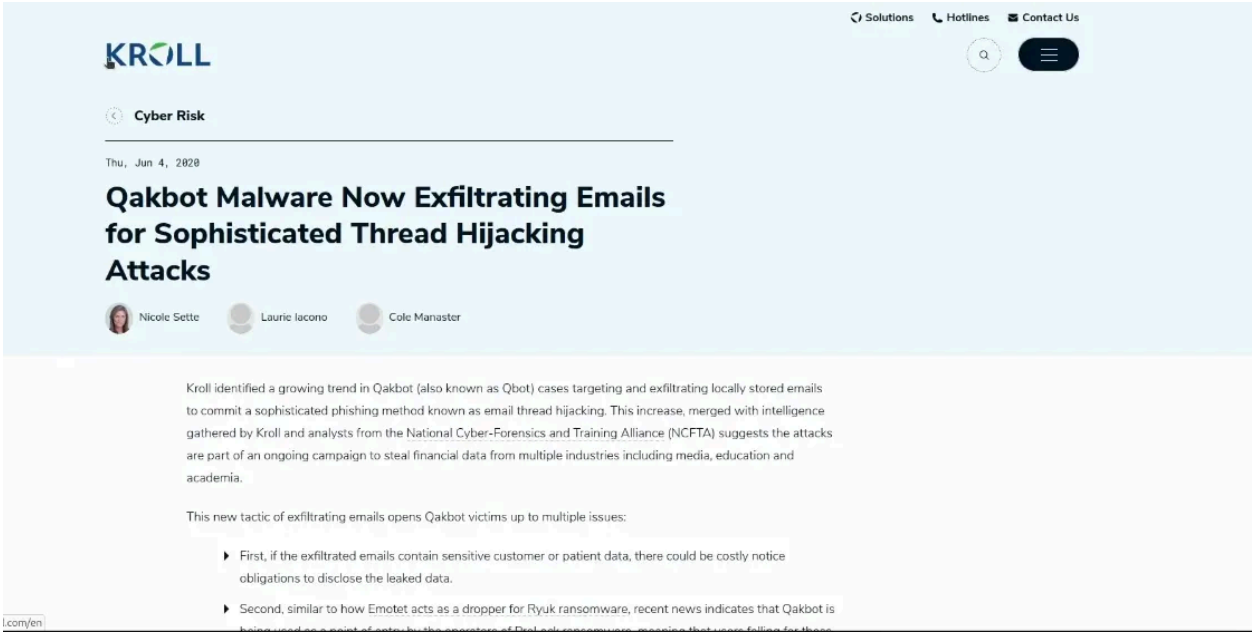
9.) Check Port scan and open port to Live IP

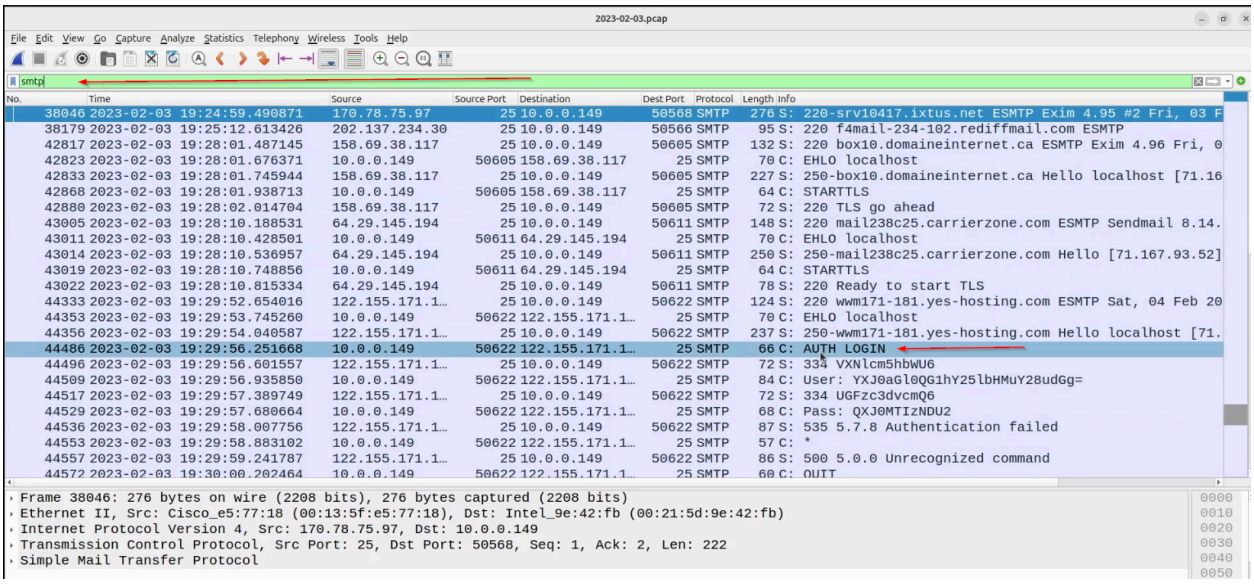
⇒ Next we check Port scan and open port perform that malware

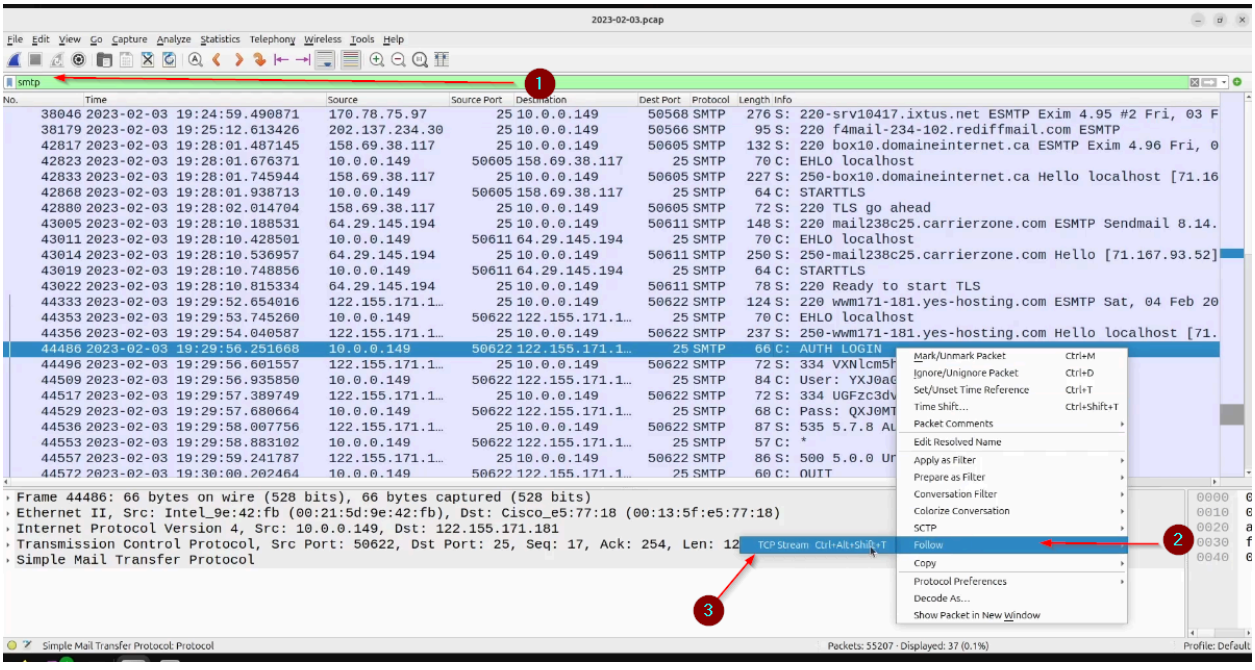
(See local 445 139 137 ports interact eternal IP that c2 server) that technique port discovery or port scan



10.) We previous analysis find that malware SMTP to steal email





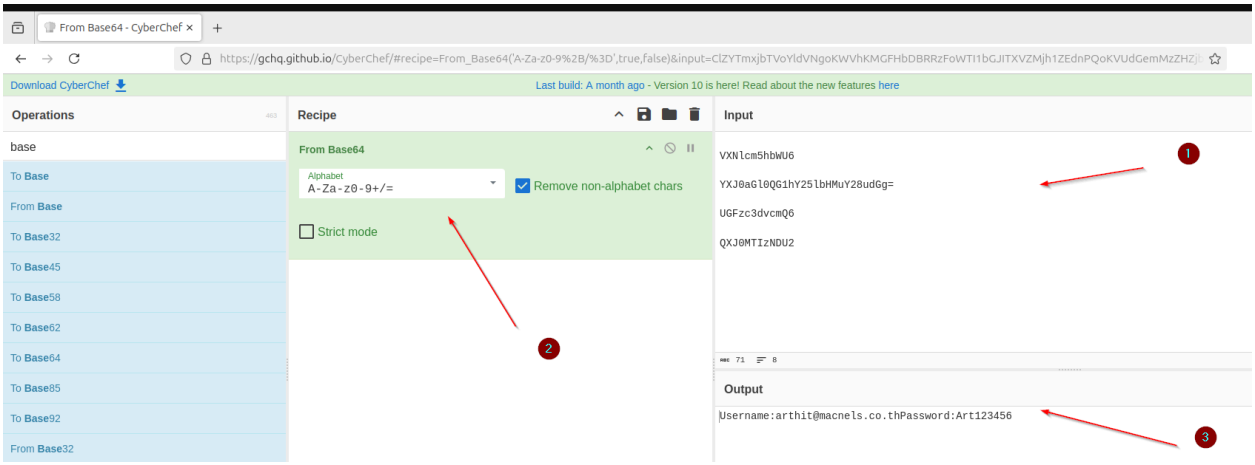


Auth login

But encode base64

Decode case use cyber chef

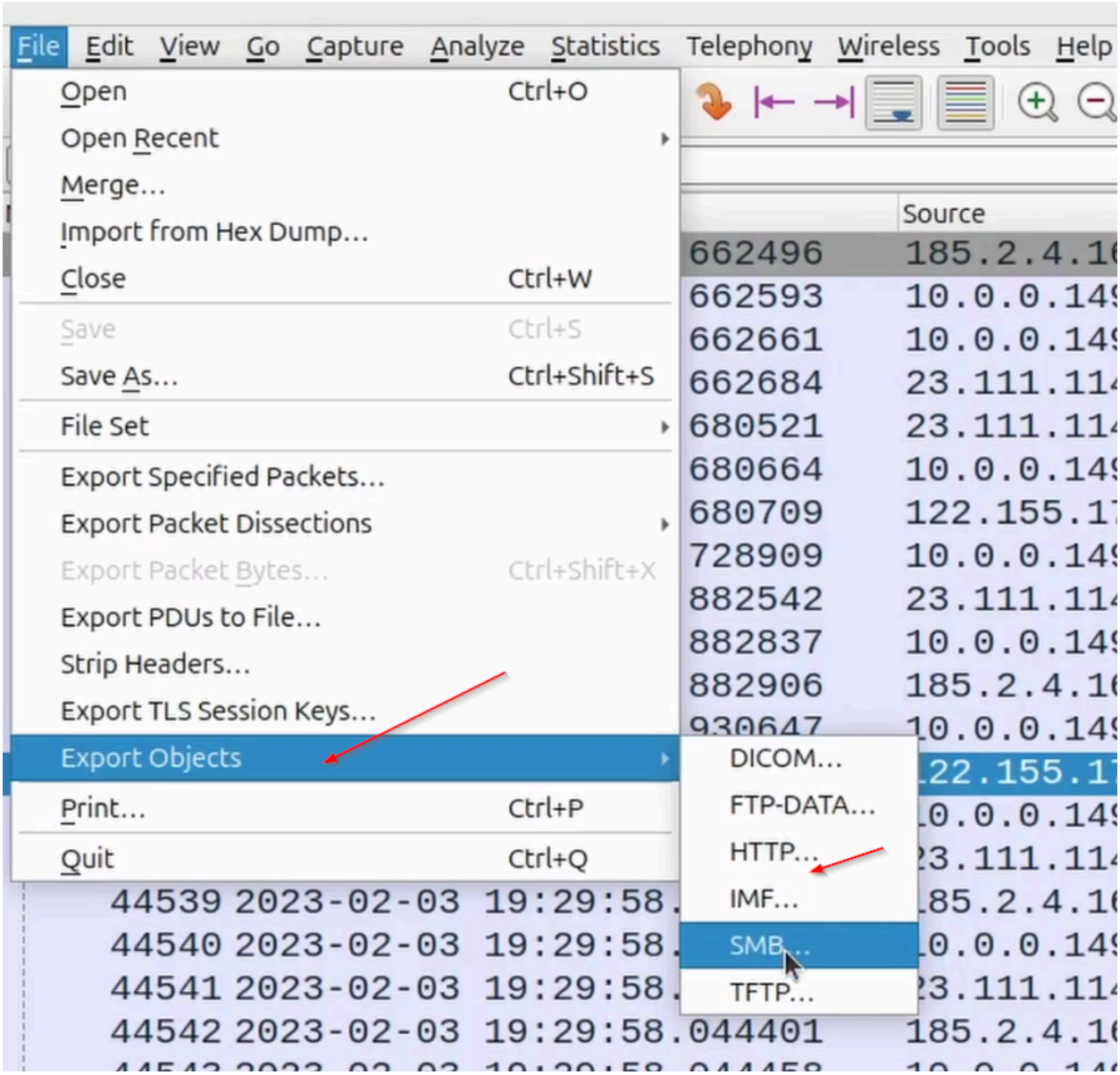
Result:

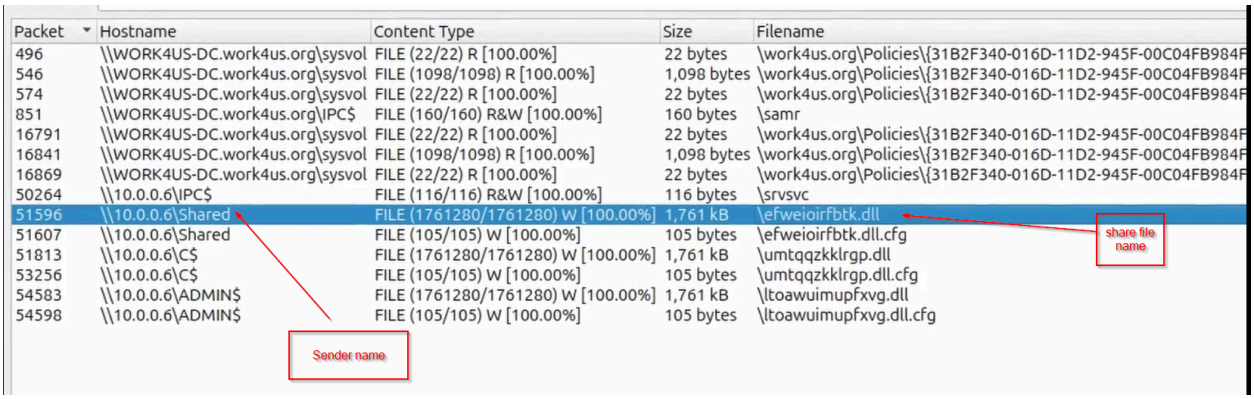


This not organization email an password

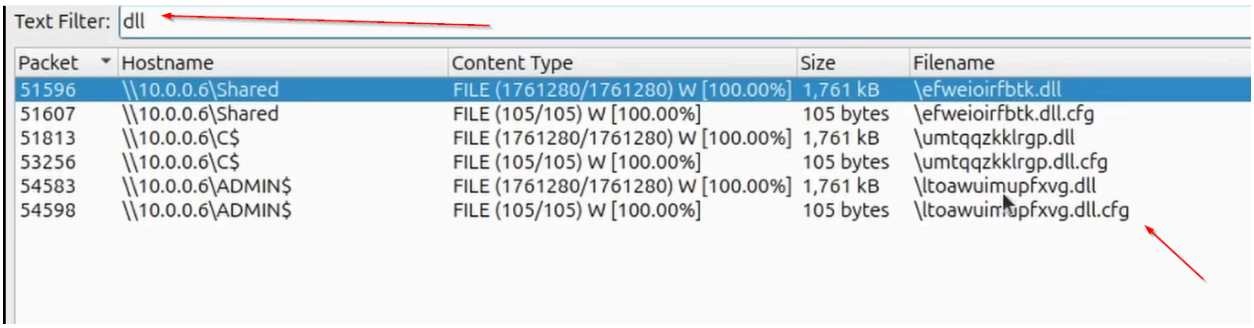
11.) SMB port open case extract information like file share happen then who and where using wireshark export object features

⇒ The
SMB object list exported from **Wireshark**. It reveals files accessed over SMB (Server Message Block), typically used for file sharing in Windows environments — very useful for analyzing **post-exploitation** activity or **lateral movement** in a network.

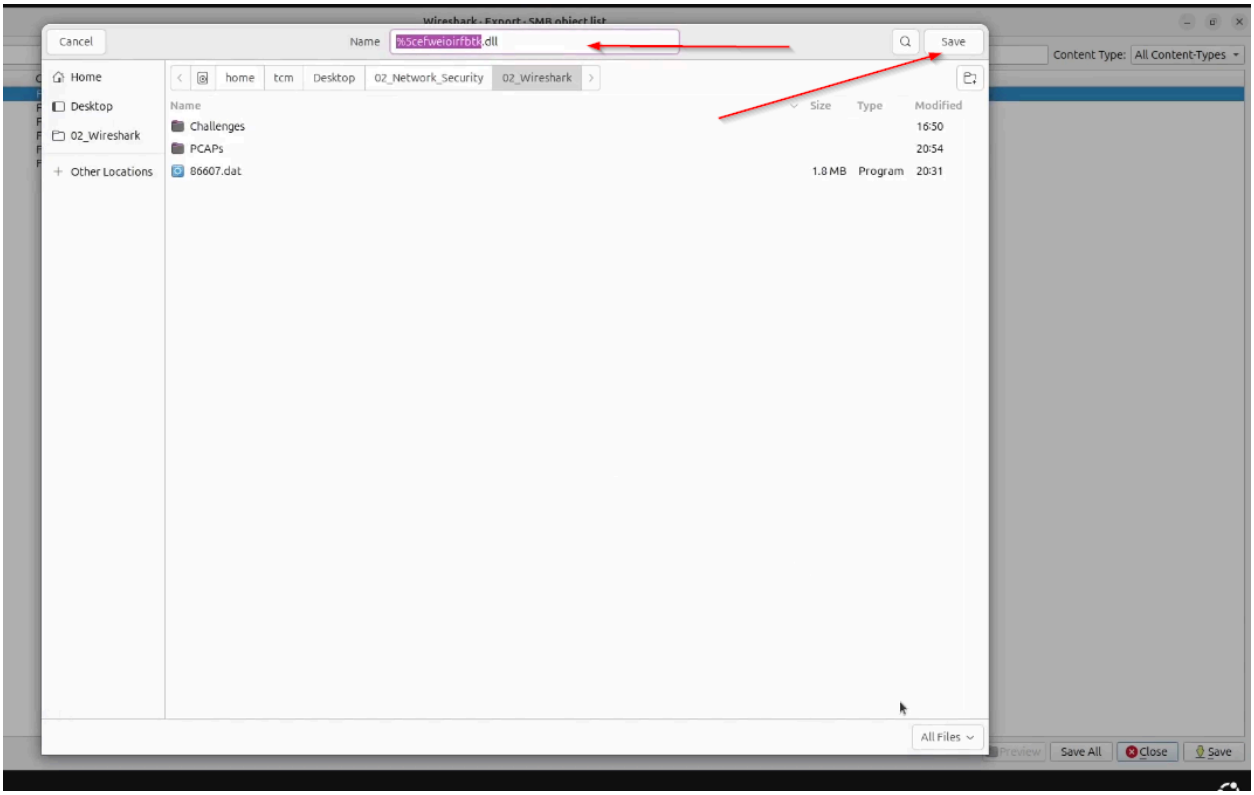

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Strip Headers...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
FTP-DATA...
HTTP...
IMF...
SMB...
TFTP...
Source
662496 185.2.4.1
662593 10.0.0.14
662661 10.0.0.14
662684 23.111.11
680521 23.111.11
680664 10.0.0.14
680709 122.155.1
728909 10.0.0.14
882542 23.111.11
882837 10.0.0.14
882906 185.2.4.1
44539 2023-02-03 19:29:58.
44540 2023-02-03 19:29:58.
44541 2023-02-03 19:29:58.
44542 2023-02-03 19:29:58.044401 185.2.4.1



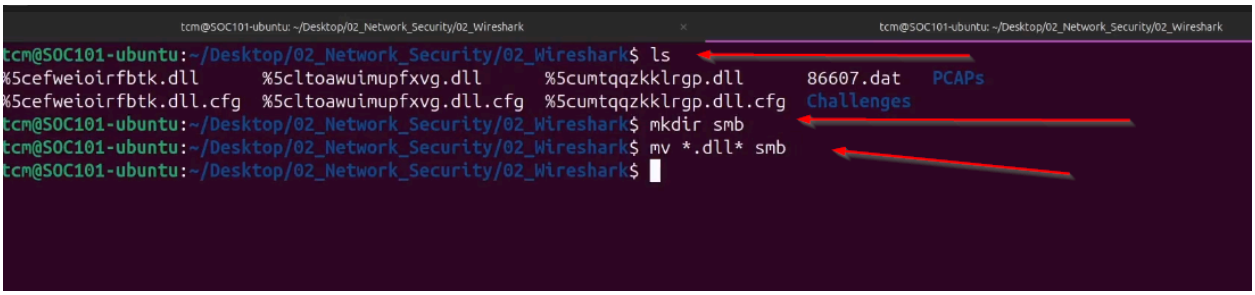
This six suspicious file

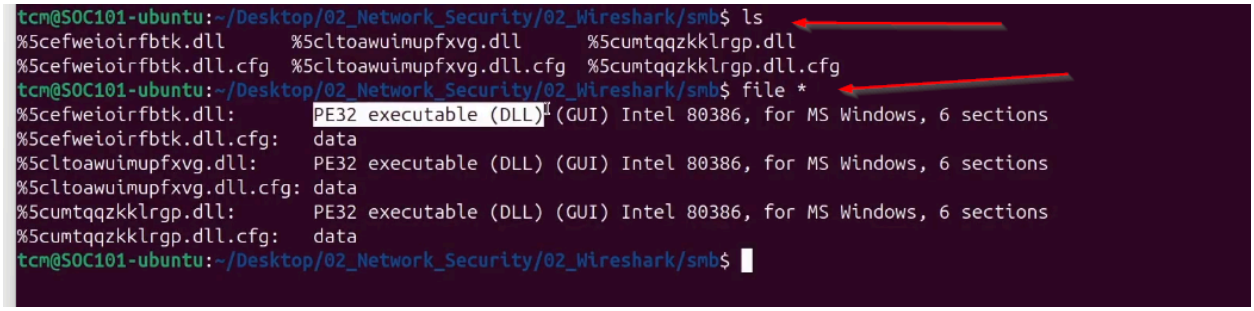


Next save that all file



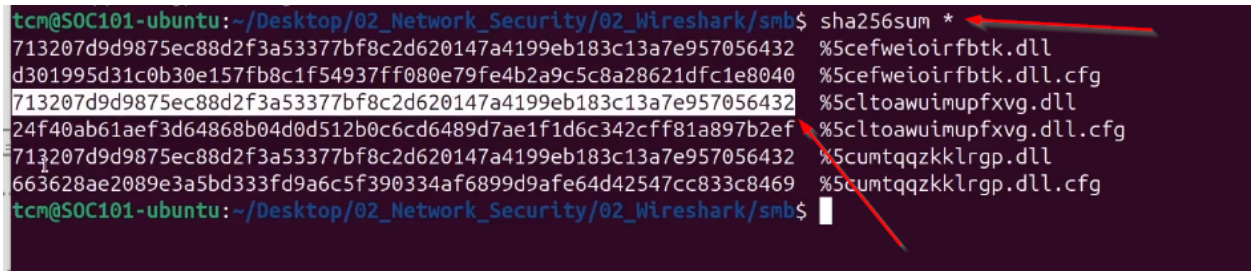
Move all file one directory and check repetition





Extract hash from download suspicious file

⇒ Note two file hash same and we found first malware qakbot also same (so check malware hash same or not same)



Next we focuses (\\10.0.0.6\Shared receiver) infected system such as SIME and EDR logs an additional PCAP analysis and what try attacker we find

Note:

⇒ We follow one IP same another live case follow same process