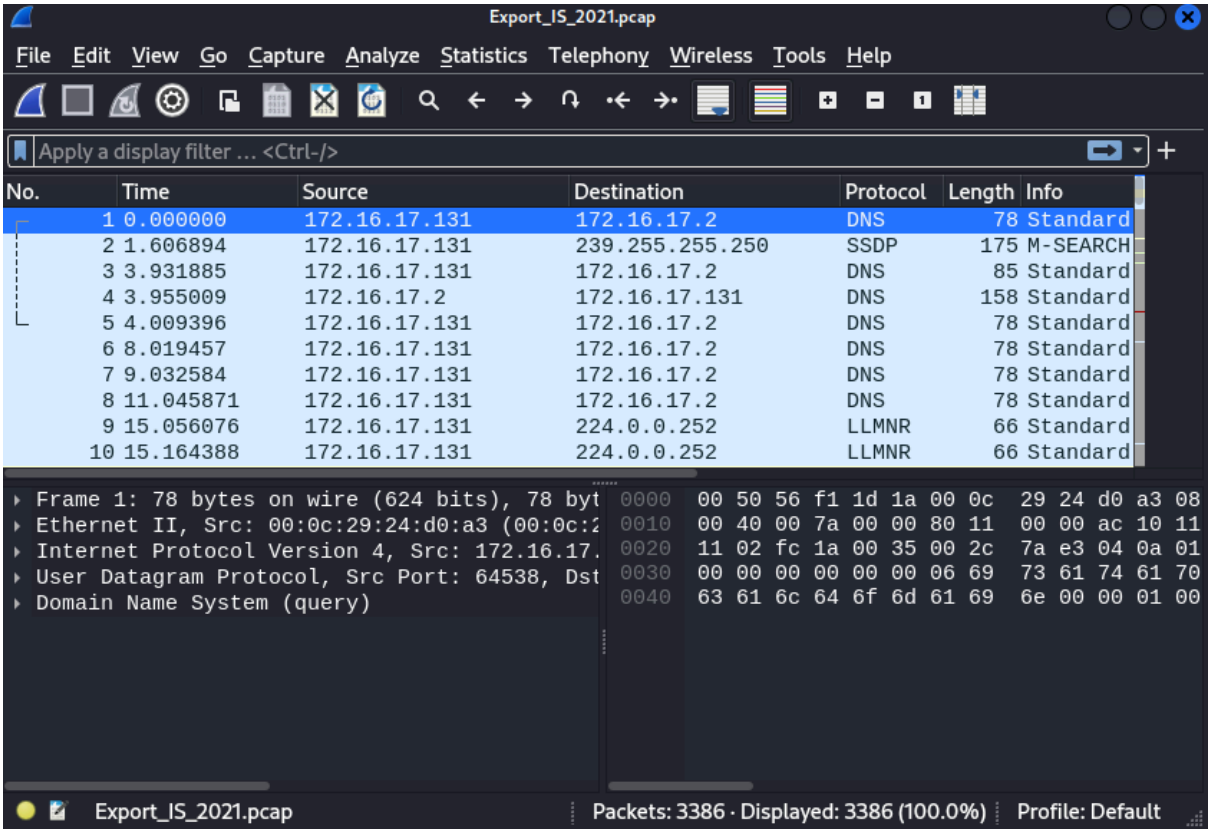
Ze względów bezpieczeństwa, usunąłem pierwsze cztery zadania, ponieważ wykonywałem tam operacje sieciowe na maszynach działających w mojej lokalnej sieci domowej.

For security reasons, I removed the first four tasks because I was performing network operations there on machines running on my local home network.

ZADANIE 5:



a) Analizie został poddany adres IPv4 172.16.17.131

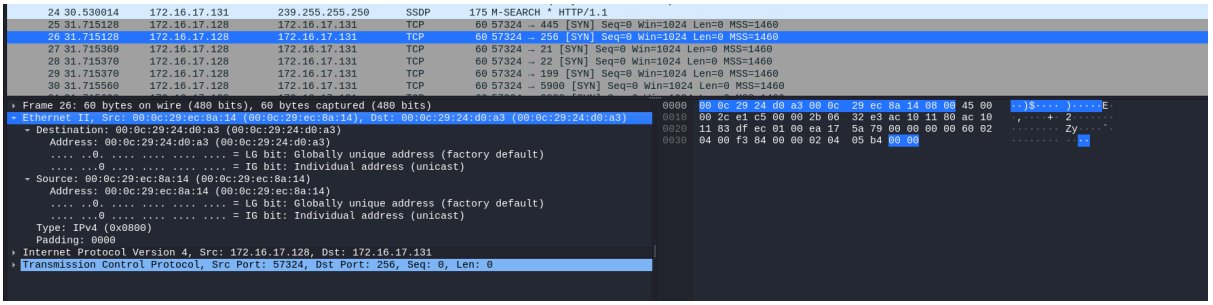
b) Gateway: 172.16.17.2

c) To działo się w ramach wirtualnych maszyn. Z przesyłanych pakietów można wyciągnąć informacje, że są to wirtualne maszyny.

d) Jesteśmy w stanie, ruch pakietów z początku pliku jest typowy dla skanowania w poszukiwaniu portów otwartych. Adres 172.16.17.131 otrzymał wiele pakietów TCP na różnych portach. Zatem ktoś szukał otwartego portu.

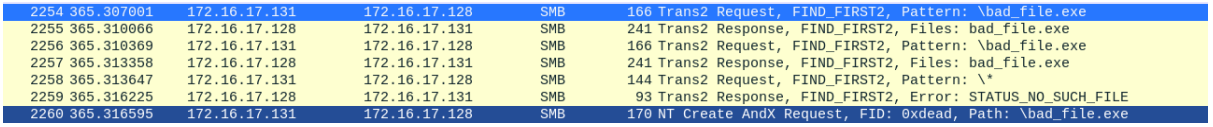
e) Atak polegał na wysyłaniu pakietów TCP na wybrane przez atakującego porty. Następnie czekał on na odpowiedź. Jeżeli odpowiedź się pojawiła, oznaczało to, że port jest otwarty.
IP: 172.17.17.128

f)

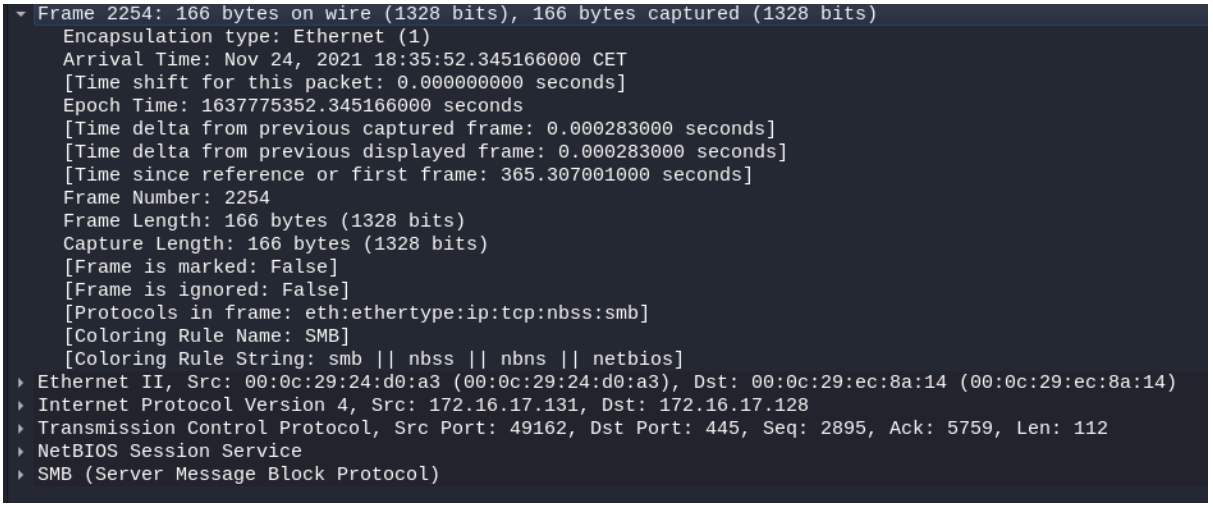


Ten adres mac należy do sprawcy ataku.

g)

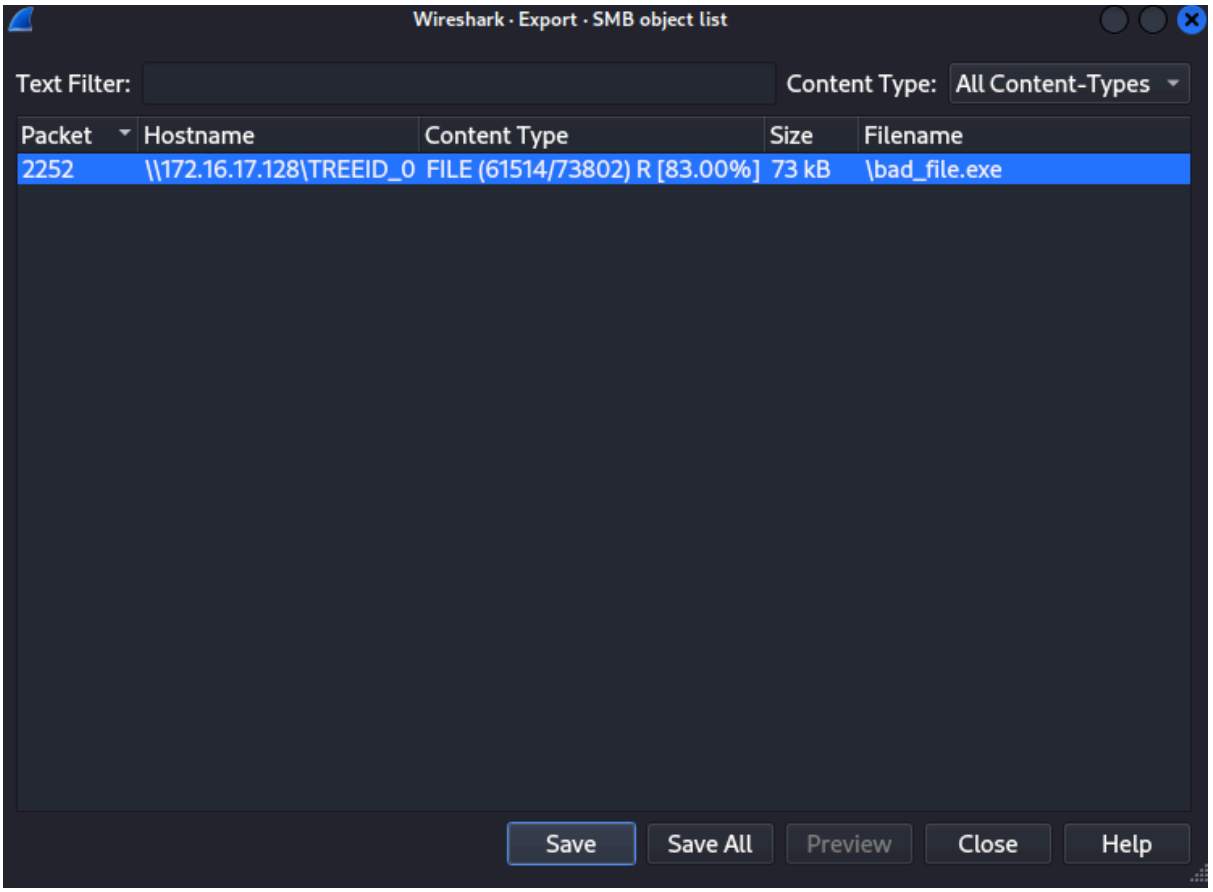


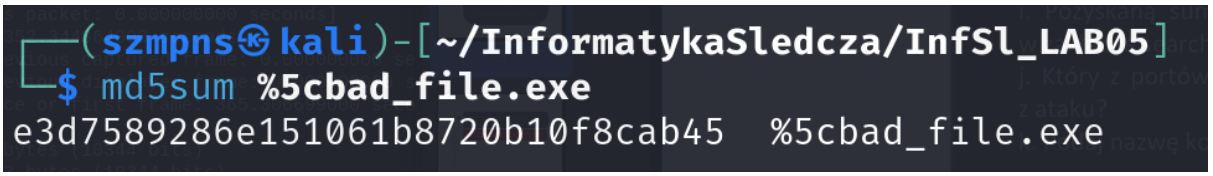
Plik nazywa się bad_file.exe



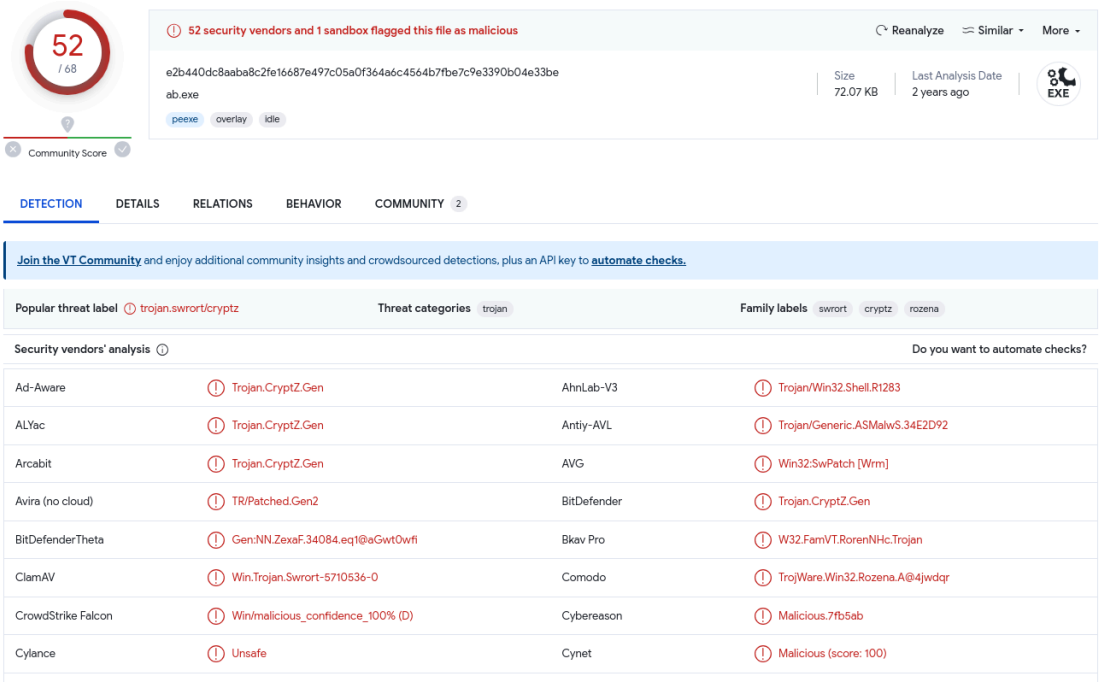
został pobrany ok. 18:35:52 z adresu atakującego(172.16.17.128), co możemy zobaczyć na 1 zrzucie ekranu.

h)





i) Z jakiegoś powodu suma została źle policzona i skrót nie istniał w bazie virus total. Inne narzędzie zrobiło to poprawnie:
f8e82827fb5ab265d6e50abce401029b



52 / 68

Community Score

52 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

e2b440dc8aaba8c2fe16687e497c05a0f364a6c4564b7fbe7c9e3390b04e33be

ab.exe

peexe overlay idle

Size 72.07 KB

Last Analysis Date 2 years ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 2

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.swrort/cryptz

Threat categories trojan

Family labels swrort cryptz rozena

Security vendors' analysis

Do you want to automate checks?

Ad-Aware	Trojan.CryptZ.Gen	AhnLab-V3	Trojan/Win32.Shell.R1283
ALYac	Trojan.CryptZ.Gen	Antiy-AVL	Trojan/Generic.ASMalwS.34E2D92
Arcabit	Trojan.CryptZ.Gen	AVG	Win32:SwPatch [Wrm]
Avira (no cloud)	TR/Patched.Gen2	BitDefender	Trojan.CryptZ.Gen
BitDefenderTheta	Gen:NN.ZexaF.34084.eq1@aGwt0wfi	Bkav Pro	W32.FamVT.RorenNHc.Trojan
ClamAV	Win.Trojan.Swrort-5710536-0	Comodo	TrojWare.Win32.Rozena.A@4jwdqr
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cybereason	Malicious.7fb5ab
Cylance	Unsafe	Cynet	Malicious (score: 100)

Ten plik zawiera bardzo wiele niebezpiecznych programów. Backdoory do 32-bitowych Windowsów oraz trojany.

Microsoft	Trojan:Win32/Meterpreter.O	NANO-Antivirus	Virus.Win32.Gen-Crypt.ccnc
Panda	Trj/GdSda.A	QuickHeal	Trojan.Swrort.A
Rising	HackTool.Swrort!1.6477 (CLASSIC)	Sangfor Engine Zero	Trojan.Win32.Save.a
SecureAge	Malicious	SentinelOne (Static ML)	Static AI - Malicious PE
Sophos	ML/PE-A + Mal/EncPk-ACE	SUPERAntiSpyware	Trojan.Backdoor-Shell
Symantec	Packed.Generic.347	TACHYON	Backdoor/W32.Agent.73802.BN
Tencent	Trojan.Win32.Cryptz.za	Trellix (FireEye)	Generic.mg.f8e82827fb5ab265
TrendMicro	Backdoor.Win32.SWRORT.SMAL01	TrendMicro-HouseCall	Backdoor.Win32.SWRORT.SMAL01
VIPRE	Trojan.Win32.Swrort.B (v)	ViRobot	Trojan.Win32.Elzob.Gen
WithSecure	Trojan.TR/Patched.Gen2	Yandex	Trojan.Rosena.Gen.1

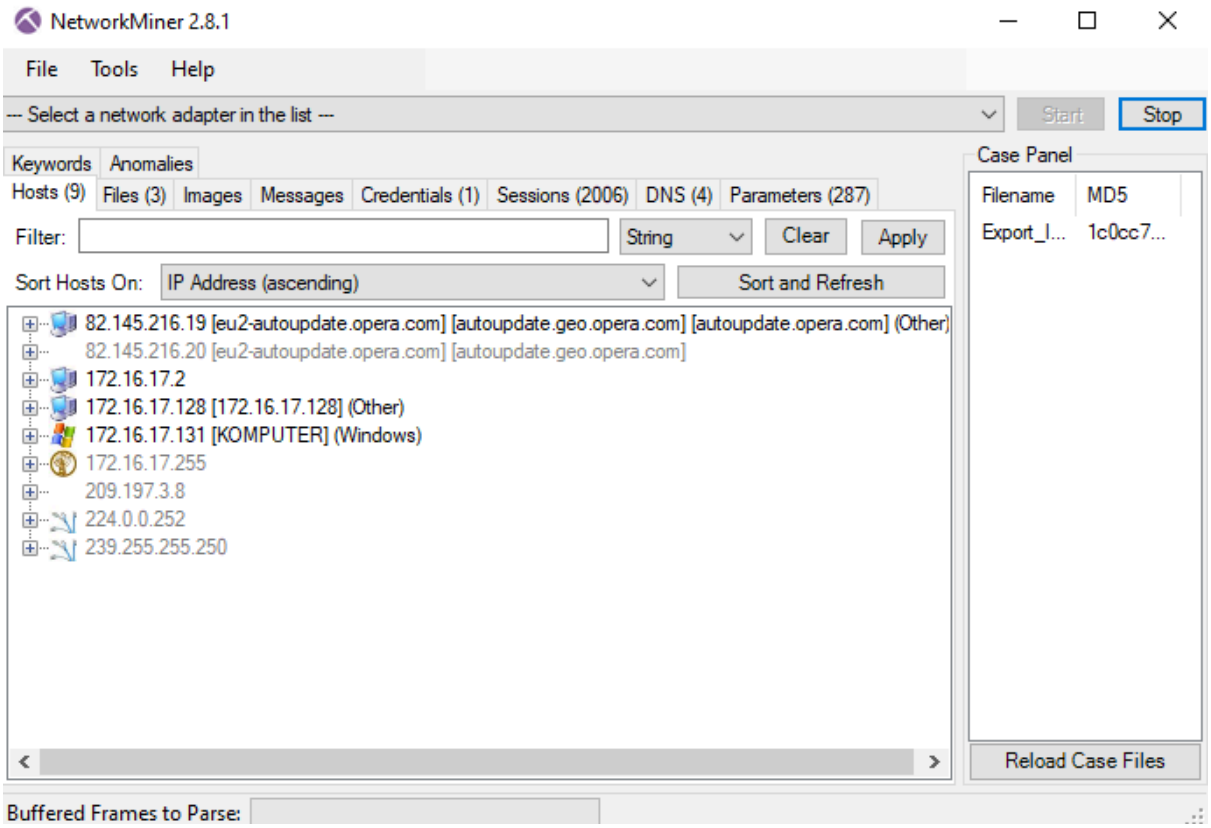
j) Był to port 49165.

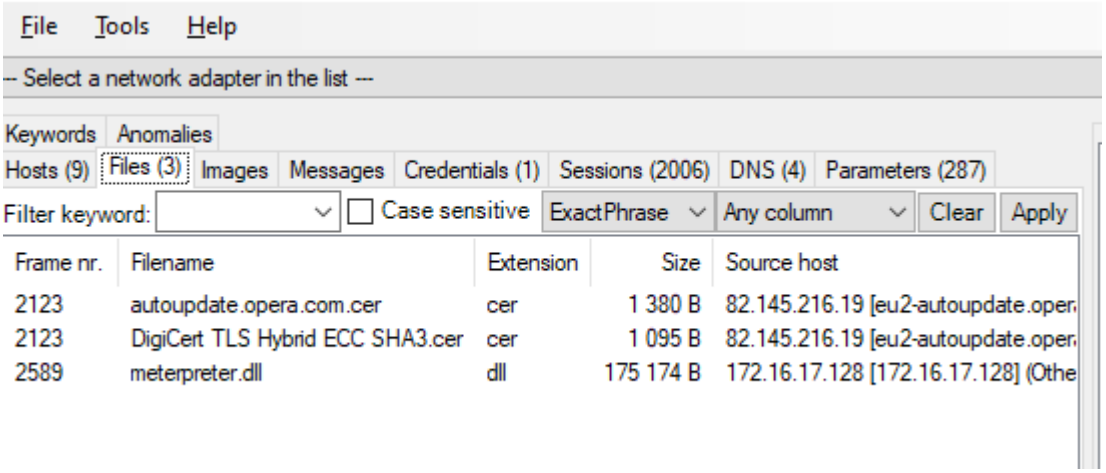
k)

1	0.000000	172.16.17.131	172.16.17.2	DNS	78 Standard query 0x040a A isatap.localdomain
2980	392.580053	172.16.17.131	172.16.17.255	BROWSER	243 Host Announcement KOMPUTER, Workstation, Server, NT Workstation
2105	152.494128	172.16.17.131	172.16.17.255	BROWSER	243 Host Announcement KOMPUTER, Workstation, Server, NT Workstation
45	32.858300	172.16.17.131	172.16.17.255	BROWSER	243 Host Announcement KOMPUTER, Workstation, Server, NT Workstation

Nazywał się KOMPUTER

ZADANIE 6:





W zakładce files nie widać tego pliku.

Plik został wysłany(informacja z analizy wireshark) za pomocą protokołu SMB, istnieje zatem szansa, że narzędzie NetworkMiner nie obsługuje w ogóle plików przesyłanych za pomocą tego protokołu.

W latach 2016-2017 podjęto kroki, aby program skuteczniej wyciągał pliki z protokołów SMB.

Po przeczytaniu kilku forów internetowych, można stwierdzić, że program ma dalej ten sam problem do dziś.

Nie pomaga nawet sugerowana zmiana uprawnień na takie, w których może zapisywać dane m.in. w pliku Assembled Files.

Program dalej ma problemy z ekstrakcją plików o rozszerzeniu .exe przesłanych za pomocą protokołu SMB.