BSidesJeddah-Part1

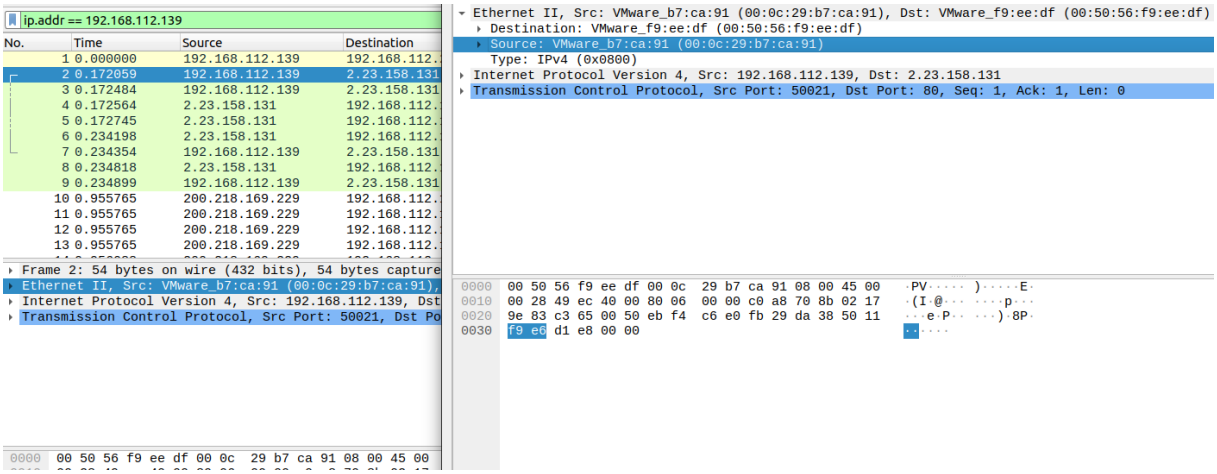
1. What is the victim's MAC address?

Wraz z plikiem pcap otrzymaliśmy plik suricata.rules który jest sygnaturami systemu IDS/IPS możemy go użyć do przeskanowania pliku pcap suricatą bądź snortem w moim przypaku suricata.

Z wygenerowanych logów możemy dowiedzieć się że adresacja ip w sieci LAN opiera się na klasie adresu C 192… dzięki tej informacji możemy wyfiltrować same adresy zaczynające się na 192.

```
michal@linux:~/Desktop/log$ cat fast.log | cut -d " " -f 21 | sort | uniq -c | sort | grep 192
     11 192.168.112.128:443
      1 192.168.112.139:110
      1 192.168.112.139:59491
      1 192.168.112.2:137
     27 192.168.112.128:80
      3 192.168.112.139:0
michal@linux:~/Desktop/log$
```

Jak można zauważyć najwięcej podejrzanego ruchu zostało zalogowane miedzy adresami 192.168.112.139 oraz 192.168.112.128 ale kiedy przyjrzymy się ruchowi w wiresharku można łatwo wywnioskować że ofiarą jest 192.168.112.139. Pozostaje odczytać jego adres fizyczny:



Answer: 00:0C:29:B7:CA:91

2. What is the address of the company associated with the victim's machine MAC address?

Dla przykładu ja użyłem tego narzędzia do znalezienia adresu:
https://www.ipchecktool.com/tool/macfinder

Answer: 3401 Hillview Avenue Palo Alto CA 94304 US

3. What is the attacker's IP address?

Uzyjemy tego polecenia aby wyfiltrować z logów suricaty wszystkie adresy oraz informacje ile razy się powtarzają i zapiszemy je do pliku out1.txt może się nam to przydać w późniejszym czasie.

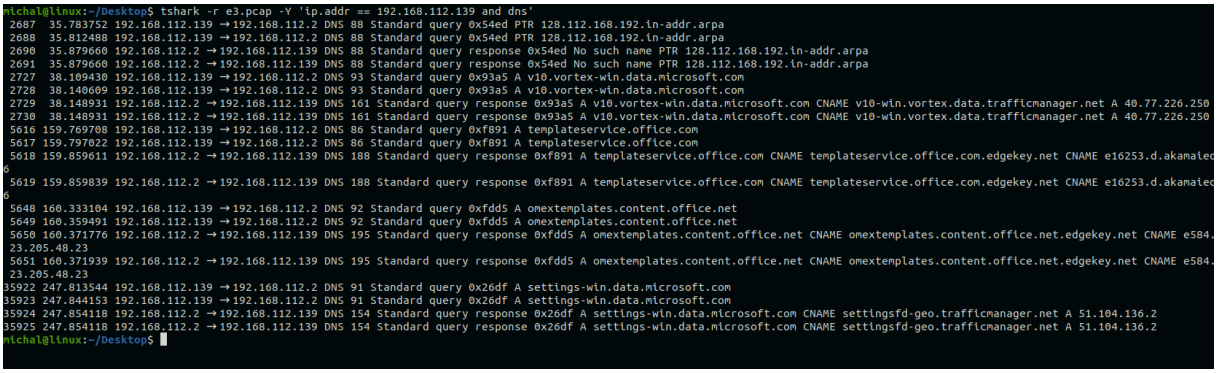
cat fast.log | cut -d " " -f 21 | sort | uniq -c | sort > out1.txt

Jeden z adresów wysyłał podejrzanie dużo ruchu do ofiary oraz wielokrotnie był uważany przez sygnatury jako potencjalna exploitacja.

Answer:192.168.112.128

4. What is the IPv4 address of the DNS server used by the victim machine?

Wyfiltrujmy ruch dns związany z adresem ip ofiary:



Jak można zaobserwować adres ofiary odpytywał tylko jeden serwer DNS

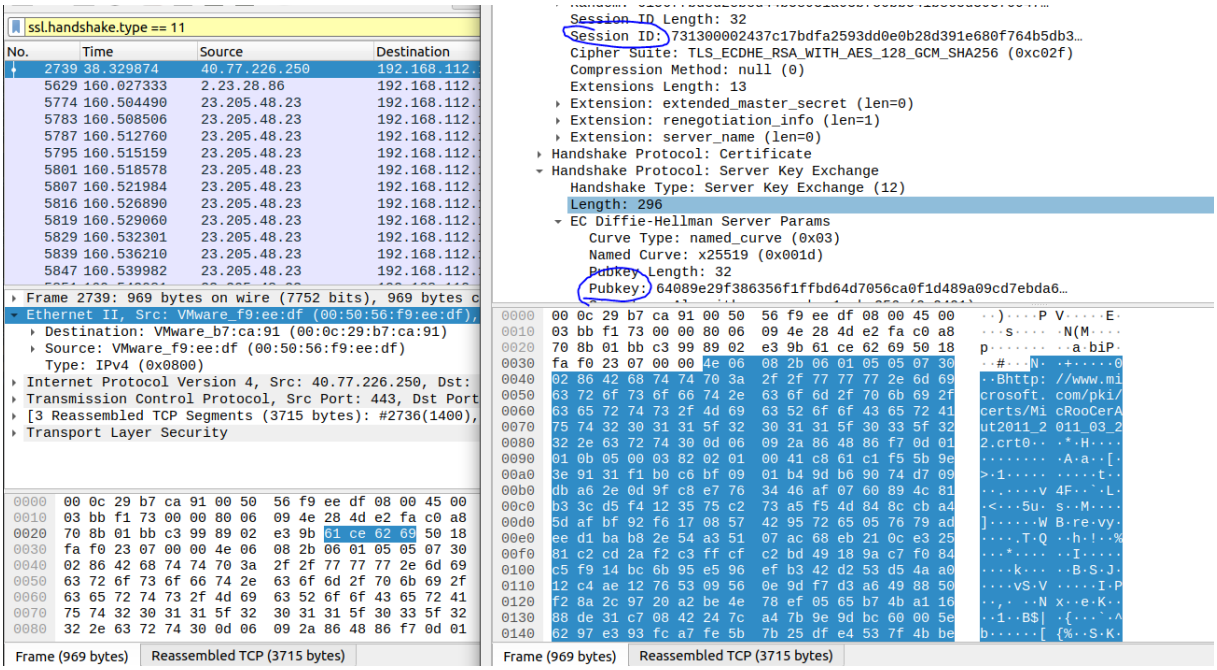
Answer:192.168.112.2

5. What domain is the victim looking up in packet 5648?

```
michal@linux:~/Desktop$ tshark -r e3.pcap -Y 'ip.addr == 192.168.112.139 and dns'
 2687  35.783752 192.168.112.139 → 192.168.112.2 DNS 88 Standard query 0x54ed PTR 128.112.168.192.in-addr.arpa
 2688  35.812488 192.168.112.139 → 192.168.112.2 DNS 88 Standard query 0x54ed PTR 128.112.168.192.in-addr.arpa
 2690  35.879660 192.168.112.2 → 192.168.112.139 DNS 88 Standard query response 0x54ed No such name PTR 128.112.168.192.in-ad
 2691  35.879660 192.168.112.2 → 192.168.112.139 DNS 88 Standard query response 0x54ed No such name PTR 128.112.168.192.in-ad
 2727  38.109430 192.168.112.139 → 192.168.112.2 DNS 93 Standard query 0x93a5 A v10.vortex-win.data.microsoft.com
 2728  38.140609 192.168.112.139 → 192.168.112.2 DNS 93 Standard query 0x93a5 A v10.vortex-win.data.microsoft.com
 2729  38.148931 192.168.112.2 → 192.168.112.139 DNS 161 Standard query response 0x93a5 A v10.vortex-win.data.microsoft.com C
 2730  38.148931 192.168.112.2 → 192.168.112.139 DNS 161 Standard query response 0x93a5 A v10.vortex-win.data.microsoft.com C
 5616 159.769708 192.168.112.139 → 192.168.112.2 DNS 86 Standard query 0xf891 A templateservice.office.com
 5617 159.797022 192.168.112.139 → 192.168.112.2 DNS 86 Standard query 0xf891 A templateservice.office.com
 5618 159.859611 192.168.112.2 → 192.168.112.139 DNS 188 Standard query response 0xf891 A templateservice.office.com CNAME te
6
 5619 159.859839 192.168.112.2 → 192.168.112.139 DNS 188 Standard query response 0xf891 A templateservice.office.com CNAME te
6
 5648 160.333104 192.168.112.139 → 192.168.112.2 DNS 92 Standard query 0xfdd5 A omextemplates.content.office.net
 5649 160.359491 192.168.112.139 → 192.168.112.2 DNS 92 Standard query 0xfdd5 A omextemplates.content.office.net
 5650 160.371776 192.168.112.2 → 192.168.112.139 DNS 195 Standard query response 0xfdd5 A omextemplates.content.office.net CN
 23.205.48.23
 5651 160.371939 192.168.112.2 → 192.168.112.139 DNS 195 Standard query response 0xfdd5 A omextemplates.content.office.net CN
 23.205.48.23
35922 247.813544 192.168.112.139 → 192.168.112.2 DNS 91 Standard query 0x26df A settings-win.data.microsoft.com
35923 247.844153 192.168.112.139 → 192.168.112.2 DNS 91 Standard query 0x26df A settings-win.data.microsoft.com
35924 247.854118 192.168.112.2 → 192.168.112.139 DNS 154 Standard query response 0x26df A settings-win.data.microsoft.com CNA
35925 247.854118 192.168.112.2 → 192.168.112.139 DNS 154 Standard query response 0x26df A settings-win.data.microsoft.com CNA
michal@linux:~/Desktop$
```

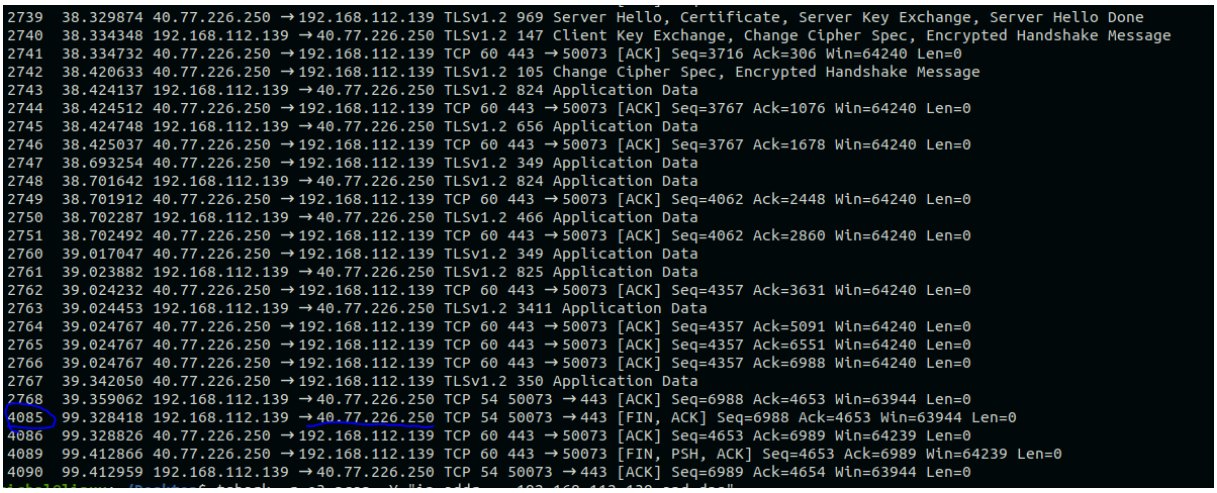
Answer: omextemplates.content.office.net

6.What is the server certificate public key that was used in TLS session: 731300002437c17bdfa2593dd0e0b28d391e680f764b5db3c4059f7abadbb28e

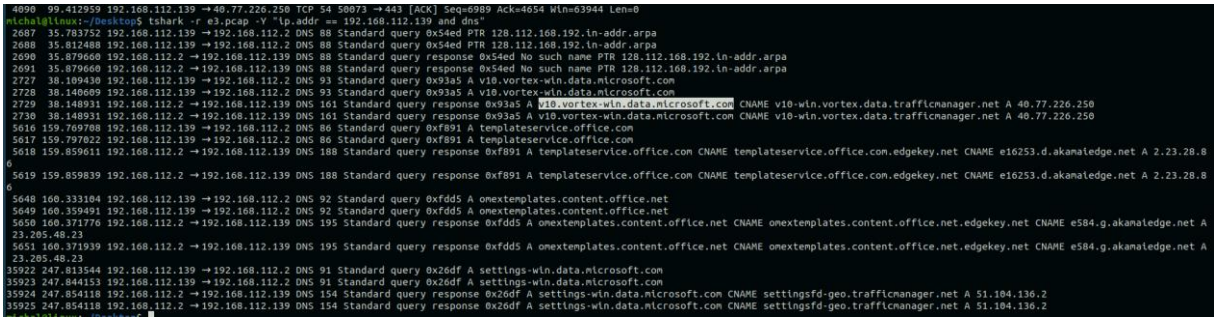


Answer: 64089e29f386356f1ffbd64d7056ca0f1d489a09cd7ebda630f2b7394e319406

7. What domain is the victim connected to in packet 4085?



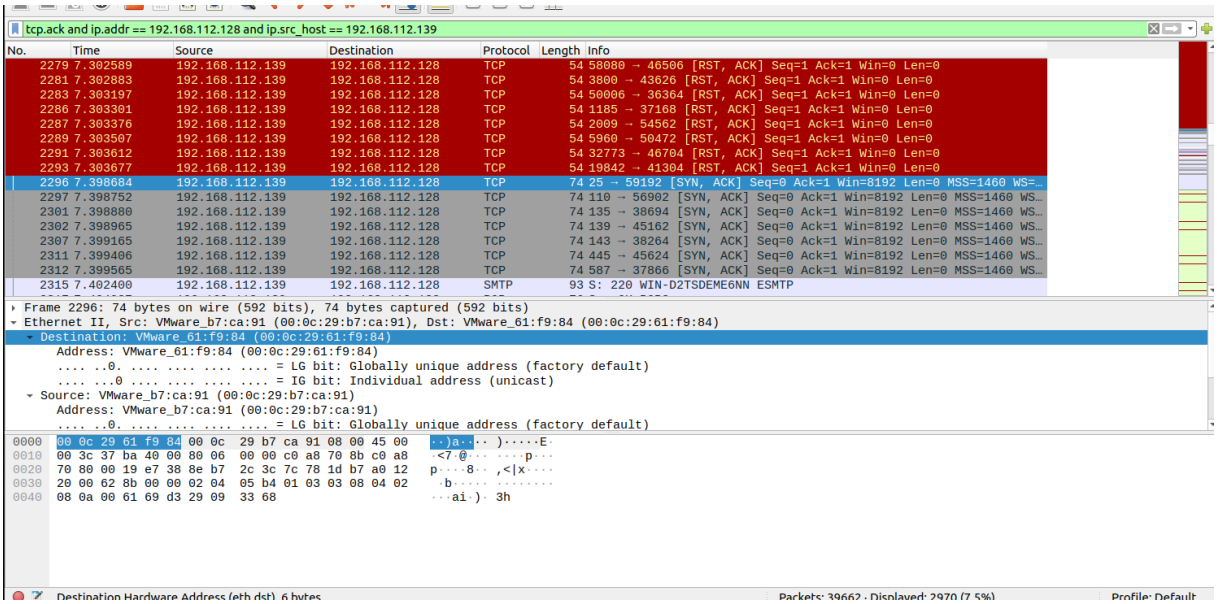
W pakiecie 4085 nasza ofiara komunikuje się z adresem 40.77.226.250 czyli z adresem logicznym ip nie mamy podanej tutaj domeny jednak kiedy wrócimy do screena z pytania 4 i 5 zauważmy że ofiara odpytywała już serwer DNS w poszukiwaniu adresu 40.77.226.250:



Answer: v10.vortex-win.data.microsoft.com

8. The attacker conducted a port scan on the victim machine. How many open ports did the attacker find?

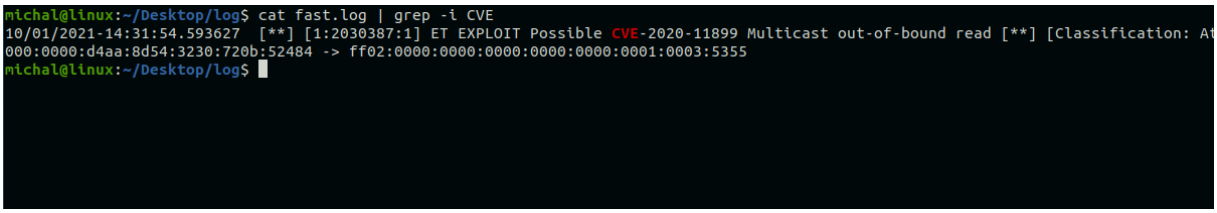
Atakujący skanował serwer / adres ofiary w poszukiwaniu otwartych portów na których działają usługi. W skrócie polega to na tymże narzędzie skanujące wysyła do określonego zakresu portów flage SYN tcp oraz oczekuje od danej usługi odpowiedzi w postaci flagi SYN, ACK



Answer:7

9. Analyze the pcap using the provided rules. What is the CVE number falsely alerted by Suricata?

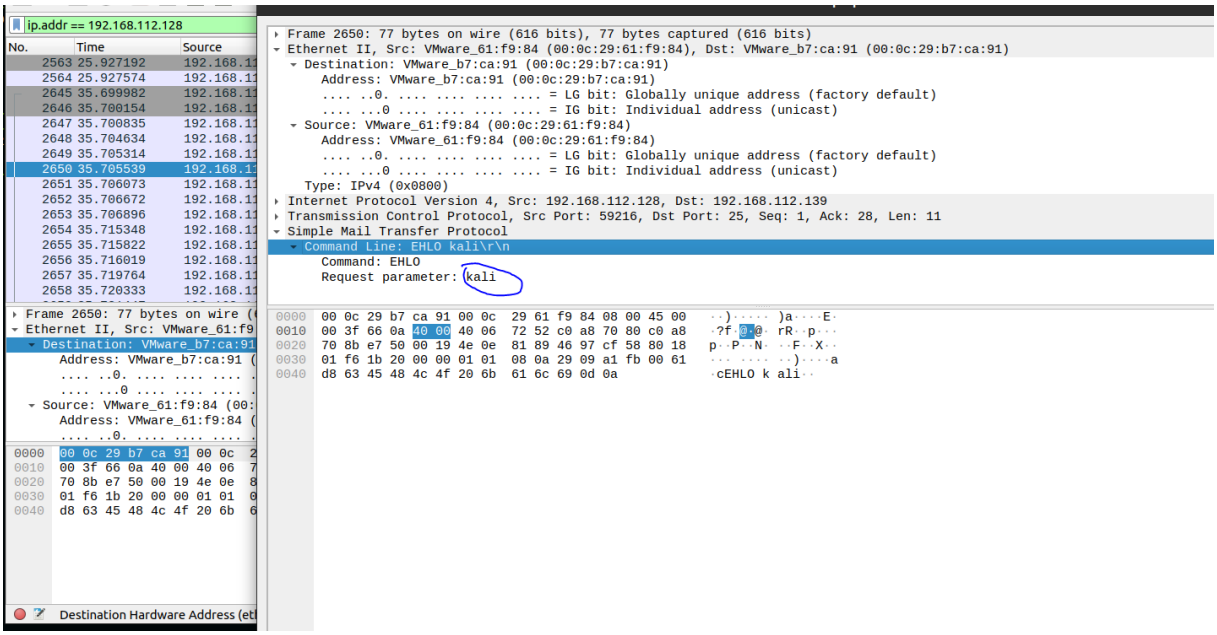
Wracamy do logów wygenerowanych przez suricate tzn fast.log oraz filtrujemy słowa kluczowego „CVE”:



Mamy jeden wynik i zawiera on poprawną odpowiedz.

Answer: CVE-2020-11899

10. What is the command parameter sent by the attacker in packet number 2650?



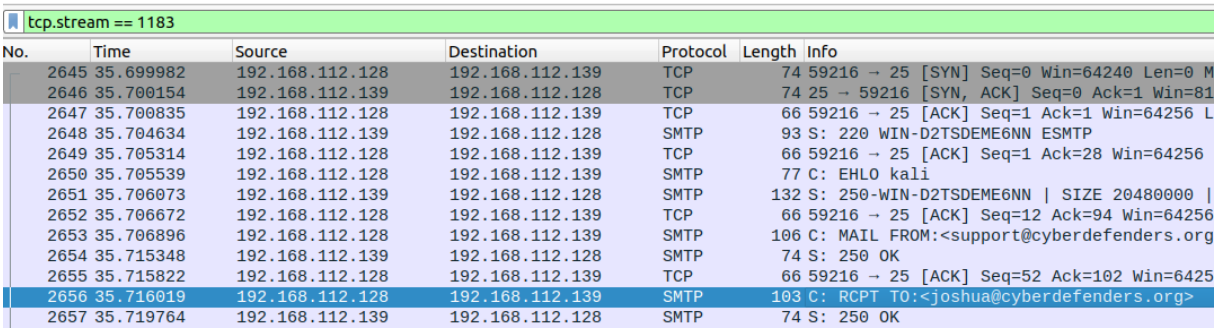
Answer: kali

11. What is the stream number which contains email traffic?

Answer:1183

12. What is the victim's email address?

Filtrujemy tcp.stream == 1183 i szukamy adresu docelowego SMTP RCPT TO:



Answer: joshua@cyberdefenders.org

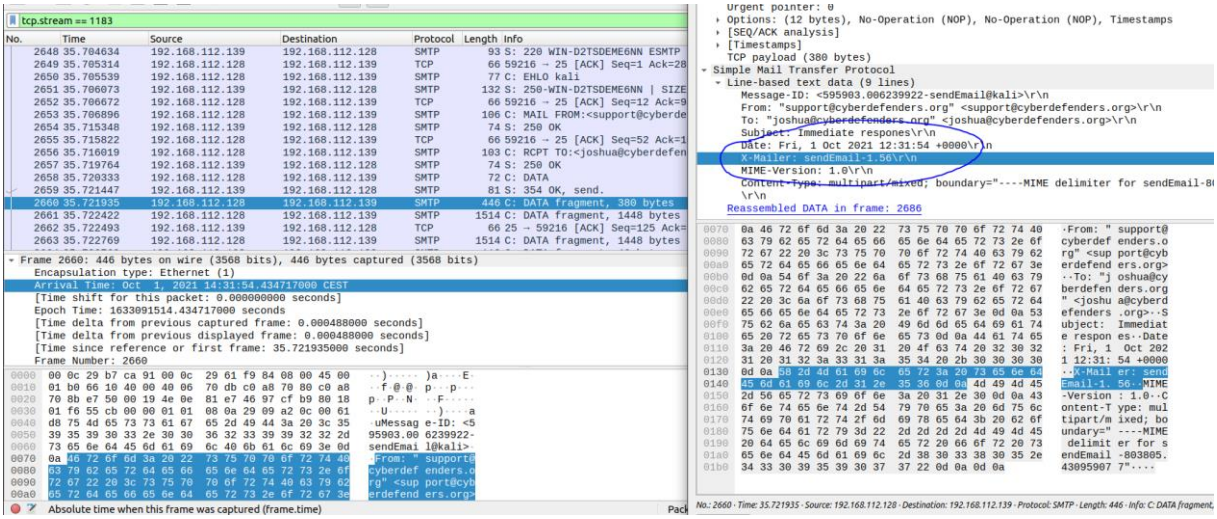
13. What was the time attacker sent the email?

Filtrujemy strumień po raz kolejny i odczytujemy godzinę z e-maila

Answer: 12:31:54

14. What is the version of the program used to send the email?

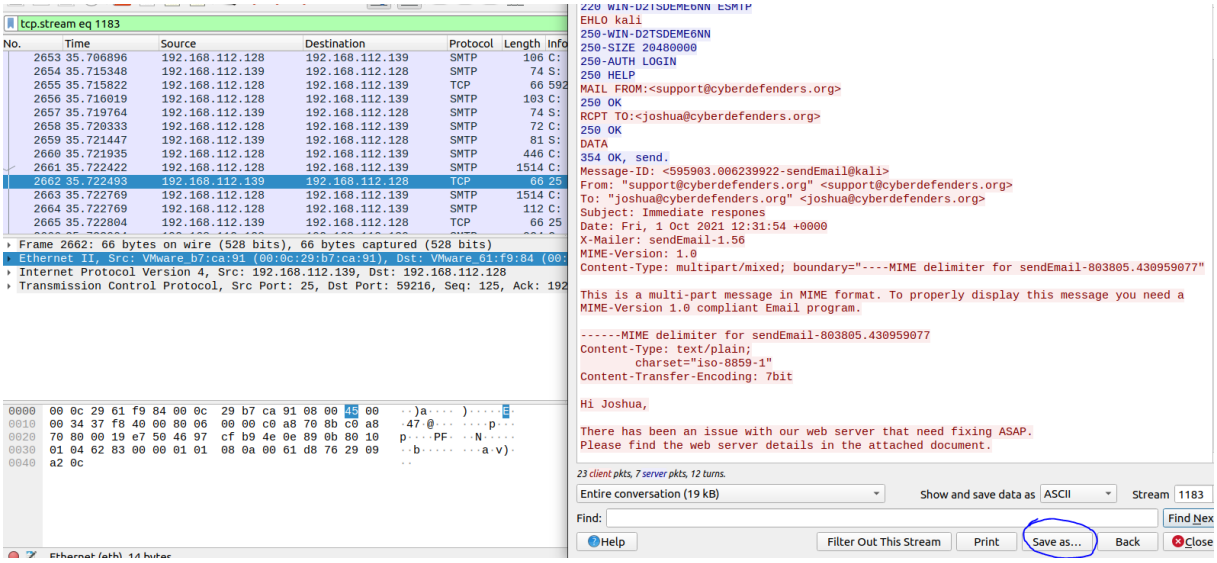
W pakiecie 2660 znajduje się zawartość wiadomości z informacji warstwy 7 można odczytać narzędzie za pomocą którego prawdopodobnie wysłano wiadomość



Answer: 1.56

15. What is the MD5 hash of the email attachment?

Robimy zrzut pakietu odpowiedzi ofiary na pakiet SMTP i zapisujemy go z rozszerzeniem .eml



Answer: 55e7660d9b21ba07fc34630d49445030

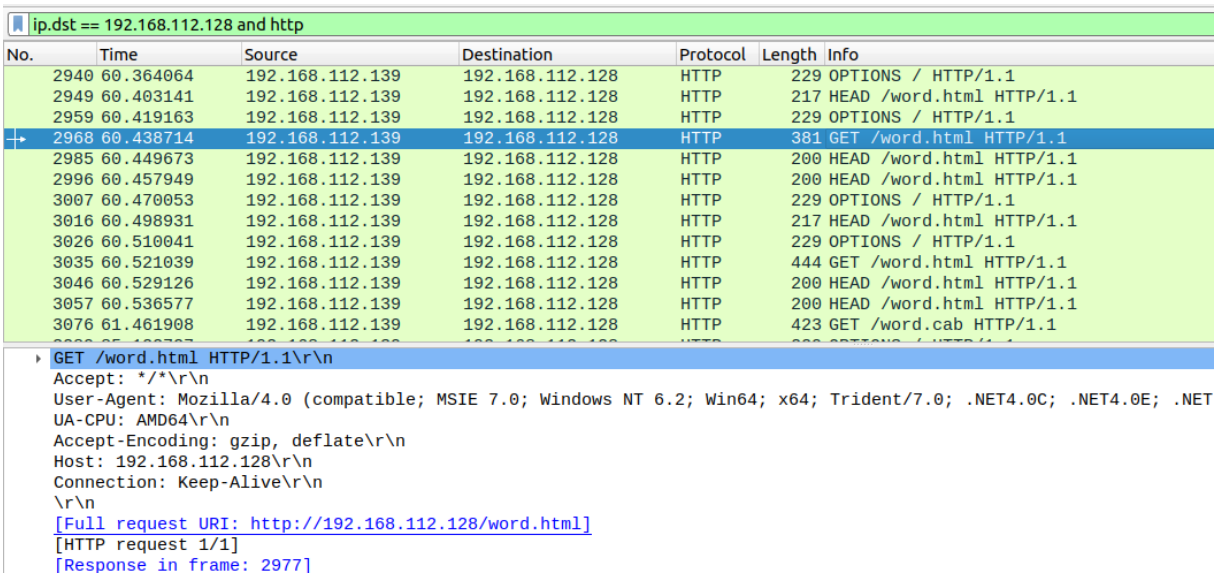
16. What is the CVE number the attacker tried to exploit using the malicious document?

Zrzucony plik wrzucamy na strone virustotal jest to sandbox zawierający silniki wielu antywirusów.

Answer: CVE-2021-40444

17. The malicious document file contains a URL to a malicious HTML file. Provide the URL for this file.

Filtrujemy w poszukiwaniu ruchu http z adresem docelowym atakującego:



Answer: http://192.168.112[.]128/word.html

20. The malicious HTML contains a js code that points to a malicious CAB file. Provide the URL to the CAB file?

Na Screenie z zadania 17 w pakiecie 3076 widzimy plik /word.cab jego lokalizacja jest bardzo podobna:

Answer: http://192.168.112[.]128/word.cab

21. The exploit takes advantage of a CAB vulnerability. Provide the vulnerability name?

Troche googlowania i odpowiedzą jest podatność ZipSlip jest to krytyczna podatność która umożliwia wykonanie kodu umieszczonego w pliku html.

Answer: ZipSlip

22. The CAB file contains a malicious dll file. What is the tool used to generate the dll?

Funkcje generowania złośliwych bibliotek dll lub innych revshelli daje np. pakiet metasploit

Answer: metasploit

23. What is the path of the dropped malicious dll file? Replace your username with IEUser

Po analizie pliku word.html i deobfuskacji możemy znaleźć lokalizacje gdzie złośliwy plik został zapisany:

Answer: C:\Users\IEUser\Appdata\Local\Temp\msword.inf

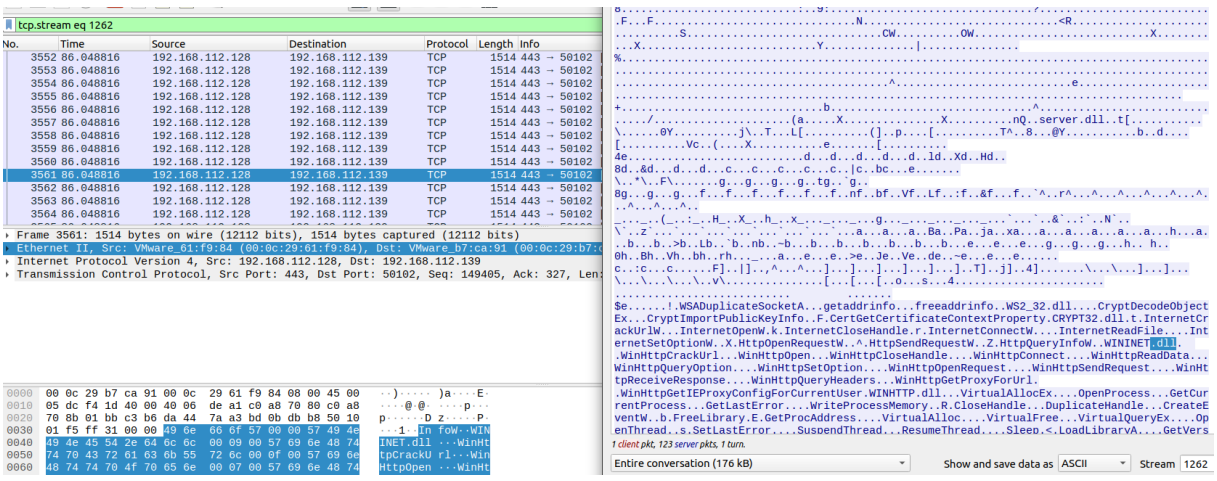
24. Analyzing the dll file what is the API used to write the shellcode in the process memory?

Możemy się tego dowiedzieć poprzez wypakowanie pliku z archiwum word.cap za pomocą polecenia: 7z e word.cab następnie sprawdzamy stringi wyodrębnionego pliku gdzie znajdujemy odpowiedz:

```
michal@linux:~/Desktop$ strings msword.inf -n 8
!This program cannot be run in DOS mode.
.text$mn
.idata$5
.rdata$zzzdbg
.idata$2
.idata$3
.idata$4
.idata$6
CloseHandle
ReleaseSemaphore
WaitForSingleObject
CreateEventA
OpenEventA
ExitThread
ResumeThread
CreateProcessA
GetThreadContext
SetThreadContext
VirtualAllocEx
WriteProcessMemory
CreateSemaphoreA
KERNEL32.dll
```

Answer: WriteProcessMemory

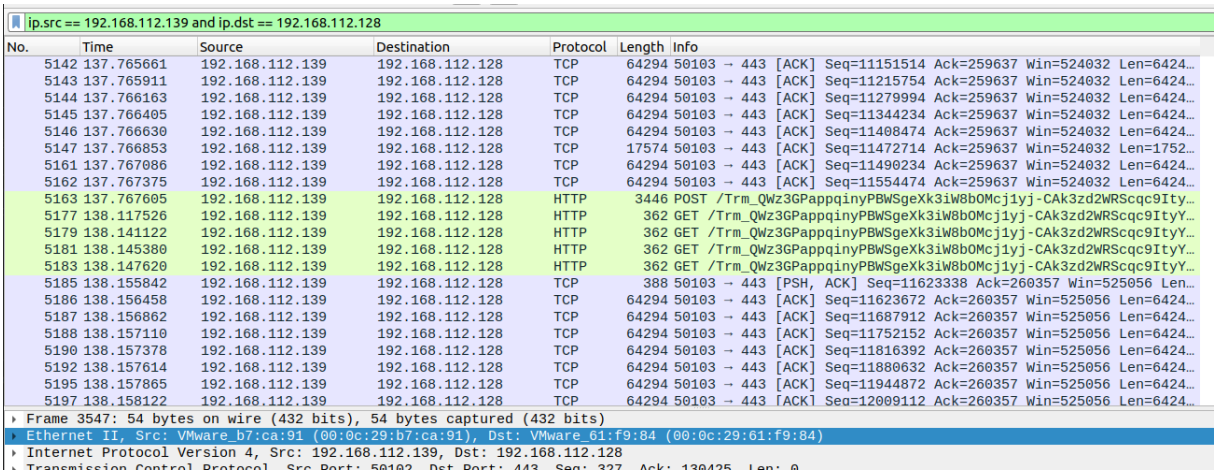
25. Extracting the shellcode from the dll file. What is the name of the library loaded by the shellcode



Adres atakującego generował bardzo dużo ruchu z portu 443 do ofiary w pakiecie 3561 można odczytać bibliotekę .dll która prawdopodobnie była załadowana do pamięci

26. Which port was configured to receive the reverse shell?

W dalszym etapie ataku adres ofiary wysyła bardzo dużo flag tcp.ack tak jakby wysyłał jakieś dane jest to typowe zachowanie revershella, Oprócz tego wysyła żądania do serwera http na adres atakującego z którego zostały wcześniej pobrane dwa złośliwe pliki



Answer: 443