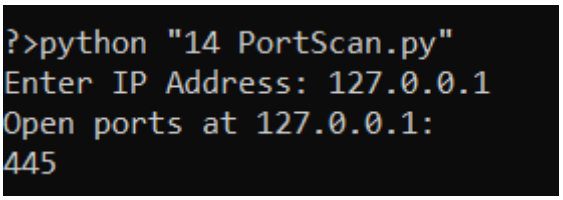
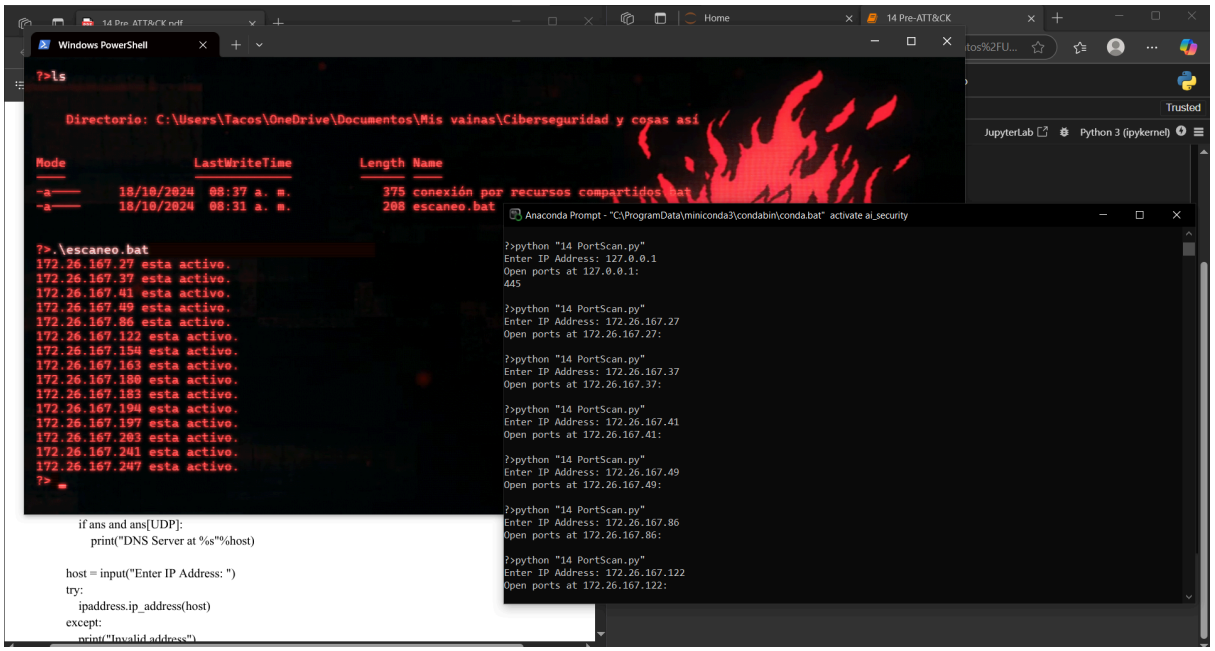
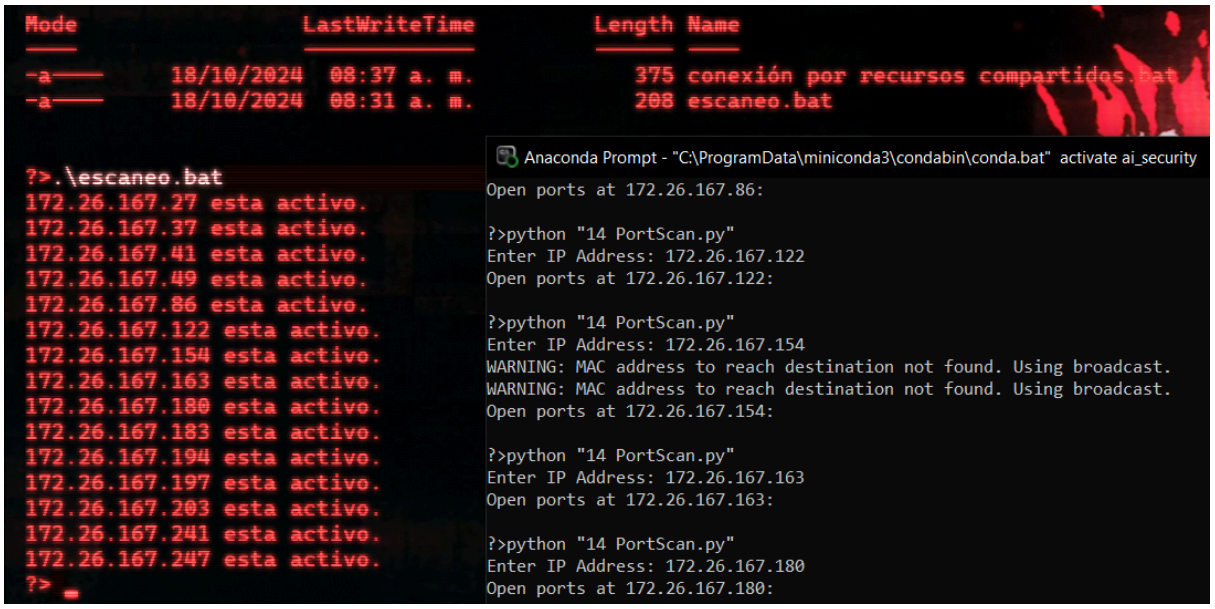
Datos, ciberseguridad e inteligencia artificial
Fecha: 20-06-2025.
Alumno: Taisen Romero Bañuelos.

Ejemplo de Pre-ATT&CK

El código de PortScan funcionó adecuadamente pese a que la mayoría de los host que descubrí con una búsqueda de host no devuelven resultados interesantes. Se adjunta el código del host discovery.







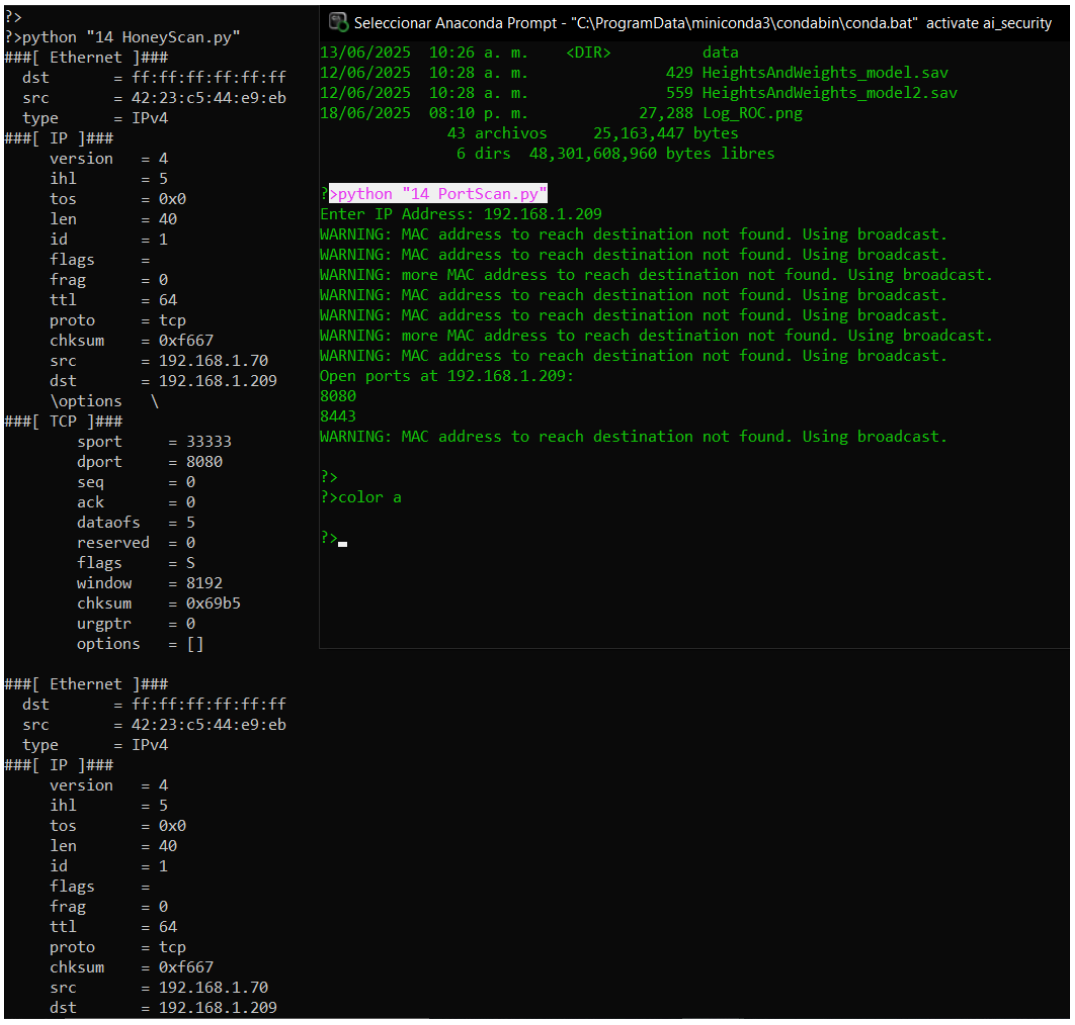
```
Mode                 LastWriteT
----                 ----------
-a----        18/10/2024  08:37 a.
-a----        18/10/2024  08:31 a.


?>.\escaneo.bat
172.26.167.27 esta activo.
172.26.167.37 esta activo.
172.26.167.41 esta activo.
172.26.167.49 esta activo.
172.26.167.86 esta activo.
172.26.167.122 esta activo.
172.26.167.154 esta activo.
172.26.167.163 esta activo.
172.26.167.180 esta activo.
172.26.167.183 esta activo.
172.26.167.194 esta activo.
172.26.167.197 esta activo.
172.26.167.203 esta activo.
172.26.167.241 esta activo.
172.26.167.247 esta activo.
?>
```

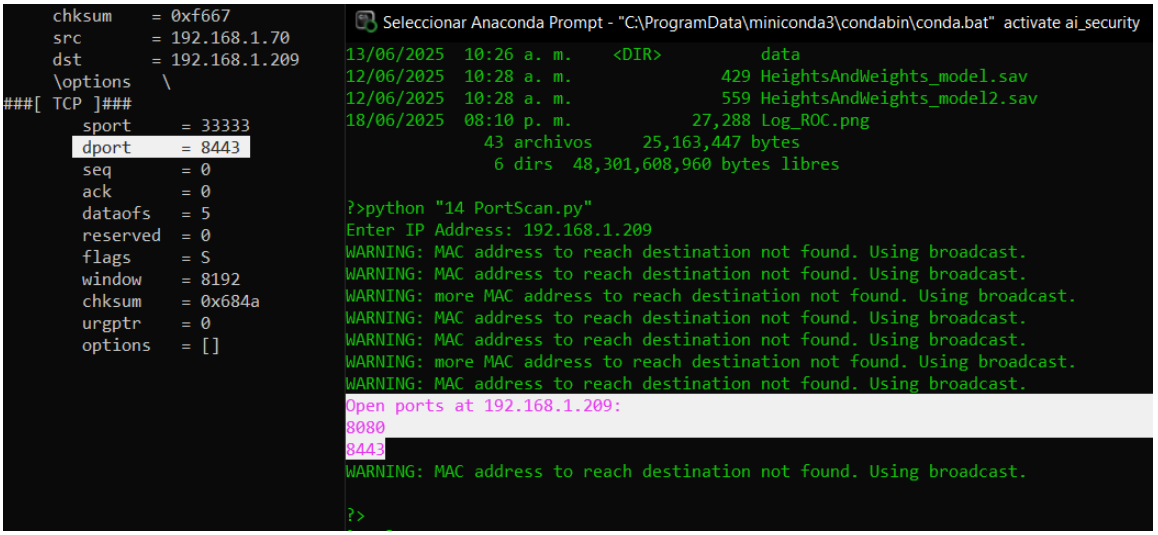
```
?>python "14 PortScan.py"
Enter IP Address: 172.26.167.194
Open ports at 172.26.167.194:

?>python "14 PortScan.py"
Enter IP Address: 172.26.167.197
Open ports at 172.26.167.197:

?>python "14 PortScan.py"
Enter IP Address: 172.26.167.203
WARNING: MAC address to reach destination not found. Using broadcast.
Open ports at 172.26.167.203:

?>python "14 PortScan.py"
Enter IP Address: 172.26.167.241
Open ports at 172.26.167.241:

?>python "14 PortScan.py"
Enter IP Address: 172.26.167.247
WARNING: MAC address to reach destination not found. Using broadcast.
WARNING: MAC address to reach destination not found. Using broadcast.
WARNING: more MAC address to reach destination not found. Using broadcast.
WARNING: MAC address to reach destination not found. Using broadcast.
WARNING: MAC address to reach destination not found. Using broadcast.
WARNING: more MAC address to reach destination not found. Using broadcast.
WARNING: MAC address to reach destination not found. Using broadcast.
Open ports at 172.26.167.247:
WARNING: MAC address to reach destination not found. Using broadcast.
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        18/10/2024  08:37 a. m.            375 conexión por recursos compartidos.bat
-a----        18/10/2024  08:31 a. m.            208 escaneo.bat


?>.\escaneo.bat
172.26.167.27 esta activo.
172.26.167.37 esta activo.
172.26.167.41 esta activo.
172.26.167.49 esta activo.
172.26.167.86 esta activo.
172.26.167.122 esta activo.
172.26.167.154 esta activo.
172.26.167.163 esta activo.
172.26.167.180 esta activo.
172.26.167.183 esta activo.
172.26.167.194 esta activo.
172.26.167.197 esta activo.
172.26.167.203 esta activo.
172.26.167.241 esta activo.
172.26.167.247 esta activo.
?> cat .\escaneo.bat
@echo off
:: Escaneo de la red local para encontrar dispositivos activos
for /L %%i in (1,1,254) do (
    ping 172.26.167.%%i -n 1 -w 100 >nul
    if not errorlevel 1 echo 172.26.167.%%i esta activo.
)
?>
```

HoneyScan

Como podemos ver, en la terminal del defensor (letras blancas) el programa HoneyScan se activa al momento de que el atacante hace la búsqueda de puertos abiertos para la IP de experimento. Se puede ver en la segunda captura como coinciden los puertos del señuelo.





DNSExploration_EDIT

Exploración DNS a Google:

```
www.google.com: ['142.250.177.4', '2607:f8b0:4012:804::2004']
tzqroa-ag-in-f4.1e100.net: ['2607:f8b0:4012:821::4']
atl14s08-in-f4.1e100.net: ['142.250.177.4']
any-in-2404.1e100.net: ['216.239.36.4']
qro02s11-in-x04.1e100.net: ['2607:f8b0:4012:804::2004']
any-in-2001-4860-4802-36--4.1e100.net: ['2001:4860:4802:36::4']
qro04s04-in-x04.1e100.net: ['2607:f8b0:4012:804::2004']
www4.google.com: ['www4.l.google.com.', '192.178.52.142', '2607:f8b0:4012:81d::200e']
tzqroa-aa-in-f14.1e100.net: ['2607:f8b0:4012:81d::e']
tzqroa-aa-in-x0e.1e100.net: ['2607:f8b0:4012:81d::200e']
www5.google.com: ['www5.l.google.com.', '192.178.52.132']
tzqroa-aa-in-f4.1e100.net: ['2607:f8b0:4012:81d::4']
www6.google.com: ['gfe.core.l.google.com.', '142.251.34.4']
qro01s27-in-f4.1e100.net: ['2607:f8b0:4012:813::4']
www9.google.com: ['2607:f8b0:4012:822::200e', '192.178.56.46', 'www3.l.google.com.']
pnqroa-ab-in-f14.1e100.net: ['192.178.56.46']
pnqroa-ab-in-x0e.1e100.net: ['2607:f8b0:4012:822::200e']
mail.google.com: ['192.178.56.197', '2607:f8b0:4012:813::2005']
```

Búsqueda DNS a la BUAP:

Edité el código original porque al ejecutarlo no me daba resultados interesantes. Comprobé con nslookup que se debía a que el subdominio portal.google.com existe en términos de DNS jerárquico, pero no tiene un registro tipo A (IPv4) asociado públicamente. Entonces decidí modificar el código para que pruebe con otro tipo de registros para buscar subdominios. Google puede tener otro tipos de registros, como CNAME, AAAA, o estar reservado internamente.

Original:

```
?>python "14 DNSExploration.py"
Traceback (most recent call last):
  File "C:\Users\Tacos\OneDrive\Documentos\Universidad\Curso - Datos, ciberseguridad e inteligencia artificial\Actividades\14 DNSExploration.py", line 57, in <module>
    HostSearch(domain,dictionary,nums)
  File "C:\Users\Tacos\OneDrive\Documentos\Universidad\Curso - Datos, ciberseguridad e inteligencia artificial\Actividades\14 DNSExploration.py", line 48, in HostSearch
    DNSRequest(d)
  File "C:\Users\Tacos\OneDrive\Documentos\Universidad\Curso - Datos, ciberseguridad e inteligencia artificial\Actividades\14 DNSExploration.py", line 25, in DNSRequest
    result = res.resolve(domain)
  File "C:\Users\Tacos\.conda\envs\ai_security\lib\site-packages\dns\resolver.py", line 1332, in resolve
    (answer, done) = resolution.query_result(response, None)
  File "C:\Users\Tacos\.conda\envs\ai_security\lib\site-packages\dns\resolver.py", line 837, in query_result
    raise NoAnswer(response=answer.response)
dns.resolver.NoAnswer: The DNS response does not contain an answer to the question: portal.google.com. IN A
```

Código modificado:

```
?>nslookup portal.google.com
Servidor:  7962v1
Address:  192.168.1.254

Nombre:  portal.google.com


?>python "14 DNSExploration_EDIT.py"
www.google.com: ['142.250.177.4', '2607:f8b0:4012:81e::2004']
tzqroa-ag-in-f4.1e100.net: ['2607:f8b0:4012:821::4']
atl14s08-in-f4.1e100.net: ['142.250.177.4']
any-in-2404.1e100.net: ['216.239.36.4']
tzqroa-ab-in-x04.1e100.net: ['2607:f8b0:4012:81e::2004']
www4.google.com: ['192.178.52.142', '2607:f8b0:4012:81d::200e', 'www4.l.google.com.']
tzqroa-aa-in-f14.1e100.net: ['2607:f8b0:4012:81d::e']
tzqroa-aa-in-x0e.1e100.net: ['2607:f8b0:4012:81d::200e']
www5.google.com: ['192.178.52.132', 'www5.l.google.com.']
tzqroa-aa-in-f4.1e100.net: ['2607:f8b0:4012:81d::4']
www6.google.com: ['gfe.core.l.google.com.', '142.251.34.4']
qro01s27-in-f4.1e100.net: ['2607:f8b0:4012:813::4']
www9.google.com: ['192.178.56.46', '2607:f8b0:4012:822::200e', 'www3.l.google.com.']
pnqroa-ab-in-f14.1e100.net: ['192.178.56.46']
pnqroa-ab-in-x0e.1e100.net: ['2607:f8b0:4012:822::200e']
mail.google.com: ['192.178.56.165', '2607:f8b0:4012:81d::2005']
pnqroa-af-in-f5.1e100.net: ['2607:f8b0:4012:826::5']
tzqroa-aa-in-x05.1e100.net: ['2607:f8b0:4012:81d::2005']
```

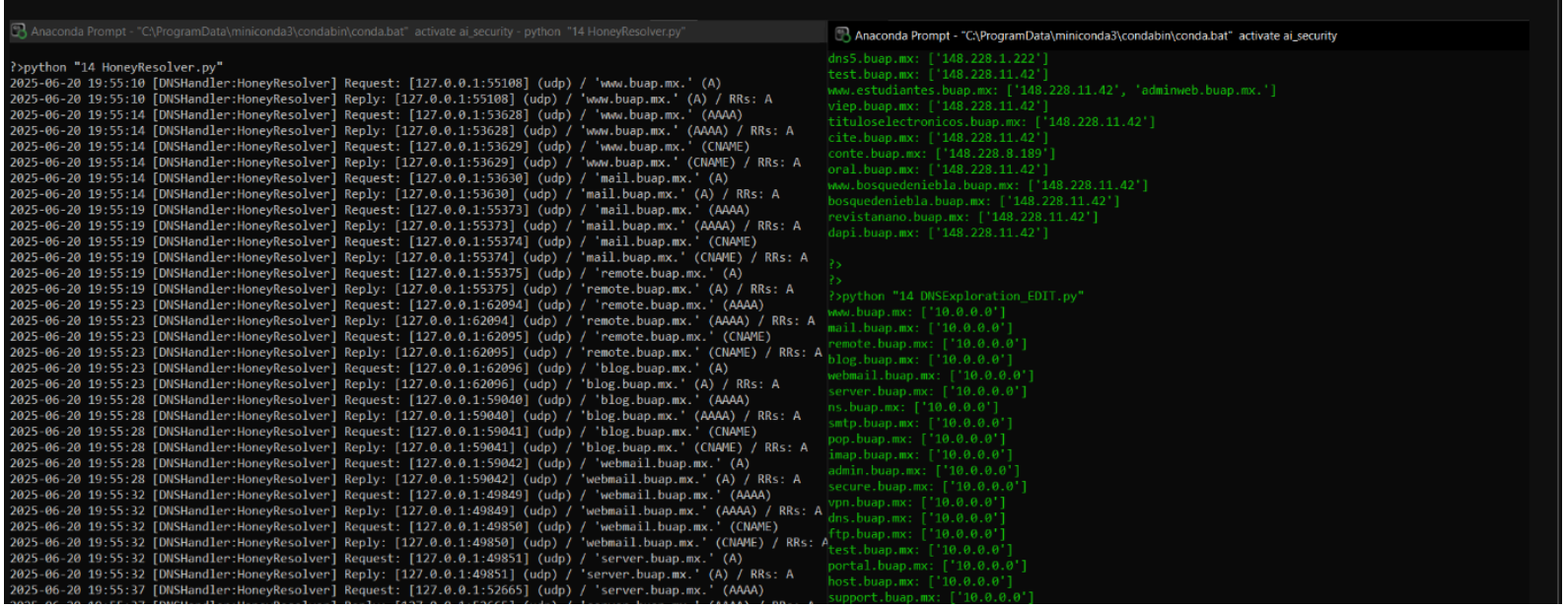
```
?>nslookup portal.buap.mx
Servidor:  7962v1
Address:  192.168.1.254

*** 7962v1 no encuentra portal.buap.mx: Non-existent domain

?>python "14 DNSExploration_EDIT.py"
www.buap.mx: ['45.60.113.125', 'eskew3g.x.incapdns.net.']
webmail.buap.mx: ['148.228.1.70', 'mx01.siu.buap.mx.']
mx01.siu.buap.mx: ['148.228.1.70']
ns1.buap.mx: ['148.228.1.100']
ns4.buap.mx: ['148.228.1.200']
dns1.buap.mx: ['148.228.1.10']
dns2.buap.mx: ['148.228.153.1']
dns3.buap.mx: ['148.228.203.14']
dns4.buap.mx: ['148.228.1.4']
dns5.buap.mx: ['148.228.1.222']
test.buap.mx: ['148.228.11.42']
www.estudiantes.buap.mx: ['148.228.11.42', 'adminweb.buap.mx.']
viep.buap.mx: ['148.228.11.42']
tituloselectronicos.buap.mx: ['148.228.11.42']
cite.buap.mx: ['148.228.11.42']
conte.buap.mx: ['148.228.8.189']
oral.buap.mx: ['148.228.11.42']
www.bosquedeniebla.buap.mx: ['148.228.11.42']
bosquedeniebla.buap.mx: ['148.228.11.42']
revistanano.buap.mx: ['148.228.11.42']
dapi.buap.mx: ['148.228.11.42']

?>
```

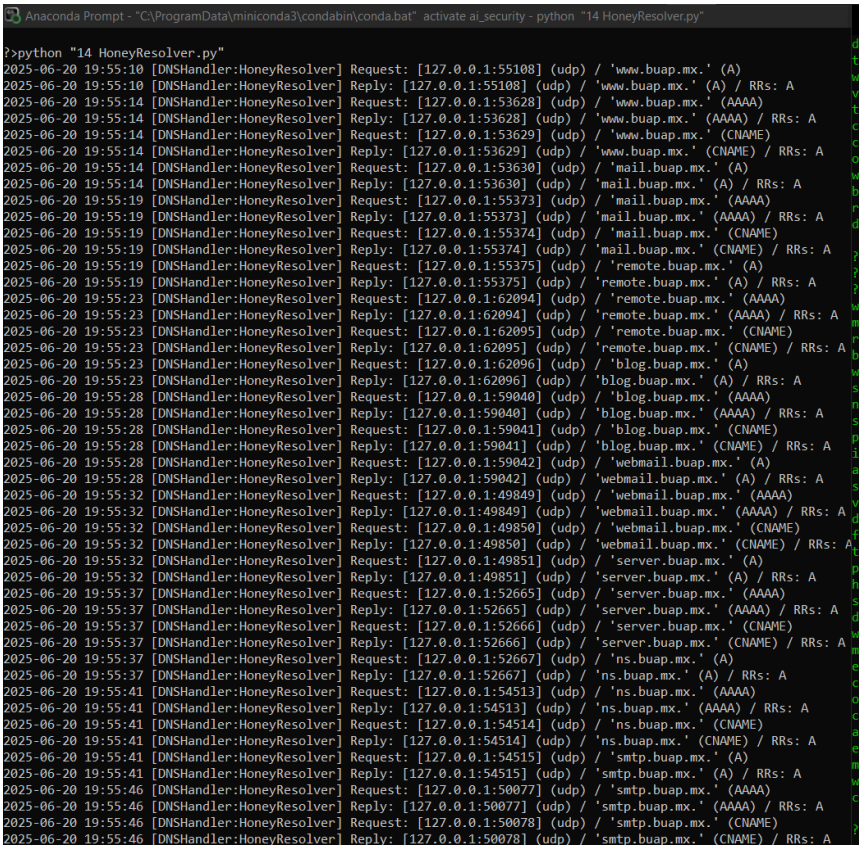
HoneyResolver

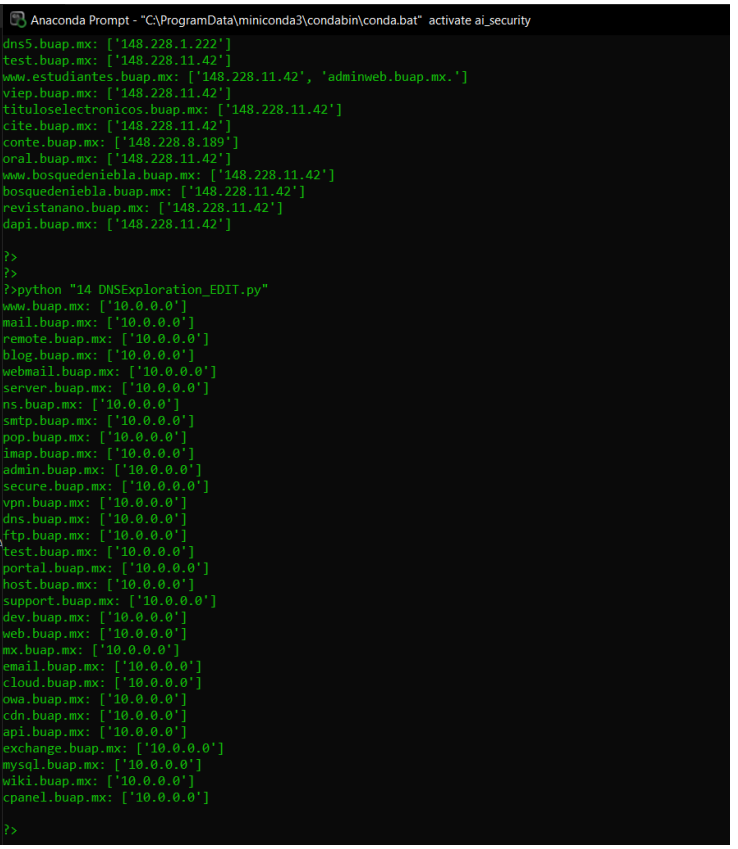
En el notebook están mis notas completas (aunque muchas notas son recordatorios de lo que me pareció importante del PDF). Para sólo mencionar los detalles relevantes mencionaré que en el archivo de DNSExploration yo no modifiqué el dominio que se iba a analizar (originalmente google.com, pero yo usé además buap.mx). Omití esa modificación porque quería experimentar y ver qué pasaba si usaba un dominio real, pues, de haber usado un dominio ficticio me hubiera perdido de una observación relevante que menciono en mis notas del notebook (véase la captura de pantalla siguiente).

Resultados:

Como se puede observar en la terminal del atacante (letras verdes), la diferencia antes y después de ejecutar el HoneyResolver es clara. No hizo falta usar un dominio ficticio (www.example.com) para poder ver lo eficaz que resulta el HoneyResolver. Pero considero que hay un detalle interesante e inesperado del que hablar, **la búsqueda de subdominios fue más exhaustiva**, esto es contraintuitivo ya que asignamos a *nums* el valor False para desactivar la búsqueda de subdominios. Mi hipótesis es que este resultado inesperado es una consecuencia de que HoneyResolver hace una "protección exhaustiva" de todos los subdominios posibles a ser atacados. Infiero esto debido a que si observamos la terminal del defensor (letras blancas) notaremos que incluso hay más subdominios que los que "descubrió" la terminal del atacante. Si bien el objetivo final del defensor fue exitoso (mostrar una misma IP para todos los subdominios) creo que hay un margen de mejora, pues sin querer le dimos más información al atacante de la que pudo obtener si no se ejecutaba el HoneyResolver (parcialmente). Esto pone de manifiesto que las soluciones de seguridad deben probarse previo a su implementación y que requieren un esfuerzo continuo de refinamiento.




Anaconda Prompt - "C:\ProgramData\miniconda3\condabin\conda.bat" activate ai_security - python "14 HoneyResolver.py"
?>python "14 HoneyResolver.py"
2025-06-20 19:55:10 [DNSHandler:HoneyResolver] Request: [127.0.0.1:55108] (udp) / 'www.buap.mx.' (A)
2025-06-20 19:55:10 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:55108] (udp) / 'www.buap.mx.' (A) / RRs: A
2025-06-20 19:55:14 [DNSHandler:HoneyResolver] Request: [127.0.0.1:53628] (udp) / 'www.buap.mx.' (AAAA)
2025-06-20 19:55:14 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:53628] (udp) / 'www.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:14 [DNSHandler:HoneyResolver] Request: [127.0.0.1:53629] (udp) / 'www.buap.mx.' (CNAME)
2025-06-20 19:55:14 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:53629] (udp) / 'www.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:14 [DNSHandler:HoneyResolver] Request: [127.0.0.1:53630] (udp) / 'mail.buap.mx.' (A)
2025-06-20 19:55:14 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:53630] (udp) / 'mail.buap.mx.' (A) / RRs: A
2025-06-20 19:55:19 [DNSHandler:HoneyResolver] Request: [127.0.0.1:55373] (udp) / 'mail.buap.mx.' (AAAA)
2025-06-20 19:55:19 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:55373] (udp) / 'mail.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:19 [DNSHandler:HoneyResolver] Request: [127.0.0.1:55374] (udp) / 'mail.buap.mx.' (CNAME)
2025-06-20 19:55:19 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:55374] (udp) / 'mail.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:19 [DNSHandler:HoneyResolver] Request: [127.0.0.1:55375] (udp) / 'remote.buap.mx.' (A)
2025-06-20 19:55:19 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:55375] (udp) / 'remote.buap.mx.' (A) / RRs: A
2025-06-20 19:55:23 [DNSHandler:HoneyResolver] Request: [127.0.0.1:62094] (udp) / 'remote.buap.mx.' (AAAA)
2025-06-20 19:55:23 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:62094] (udp) / 'remote.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:23 [DNSHandler:HoneyResolver] Request: [127.0.0.1:62095] (udp) / 'remote.buap.mx.' (CNAME)
2025-06-20 19:55:23 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:62095] (udp) / 'remote.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:23 [DNSHandler:HoneyResolver] Request: [127.0.0.1:62096] (udp) / 'blog.buap.mx.' (A)
2025-06-20 19:55:23 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:62096] (udp) / 'blog.buap.mx.' (A) / RRs: A
2025-06-20 19:55:28 [DNSHandler:HoneyResolver] Request: [127.0.0.1:59040] (udp) / 'blog.buap.mx.' (AAAA)
2025-06-20 19:55:28 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:59040] (udp) / 'blog.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:28 [DNSHandler:HoneyResolver] Request: [127.0.0.1:59041] (udp) / 'blog.buap.mx.' (CNAME)
2025-06-20 19:55:28 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:59041] (udp) / 'blog.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:28 [DNSHandler:HoneyResolver] Request: [127.0.0.1:59042] (udp) / 'webmail.buap.mx.' (A)
2025-06-20 19:55:28 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:59042] (udp) / 'webmail.buap.mx.' (A) / RRs: A
2025-06-20 19:55:32 [DNSHandler:HoneyResolver] Request: [127.0.0.1:49849] (udp) / 'webmail.buap.mx.' (AAAA)
2025-06-20 19:55:32 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:49849] (udp) / 'webmail.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:32 [DNSHandler:HoneyResolver] Request: [127.0.0.1:49850] (udp) / 'webmail.buap.mx.' (CNAME)
2025-06-20 19:55:32 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:49850] (udp) / 'webmail.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:32 [DNSHandler:HoneyResolver] Request: [127.0.0.1:49851] (udp) / 'server.buap.mx.' (A)
2025-06-20 19:55:32 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:49851] (udp) / 'server.buap.mx.' (A) / RRs: A
2025-06-20 19:55:37 [DNSHandler:HoneyResolver] Request: [127.0.0.1:52665] (udp) / 'server.buap.mx.' (AAAA)
2025-06-20 19:55:37 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:52665] (udp) / 'server.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:37 [DNSHandler:HoneyResolver] Request: [127.0.0.1:52666] (udp) / 'server.buap.mx.' (CNAME)
2025-06-20 19:55:37 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:52666] (udp) / 'server.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:37 [DNSHandler:HoneyResolver] Request: [127.0.0.1:52667] (udp) / 'ns.buap.mx.' (A)
2025-06-20 19:55:37 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:52667] (udp) / 'ns.buap.mx.' (A) / RRs: A
2025-06-20 19:55:41 [DNSHandler:HoneyResolver] Request: [127.0.0.1:54513] (udp) / 'ns.buap.mx.' (AAAA)
2025-06-20 19:55:41 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:54513] (udp) / 'ns.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:41 [DNSHandler:HoneyResolver] Request: [127.0.0.1:54514] (udp) / 'ns.buap.mx.' (CNAME)
2025-06-20 19:55:41 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:54514] (udp) / 'ns.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:41 [DNSHandler:HoneyResolver] Request: [127.0.0.1:54515] (udp) / 'smtp.buap.mx.' (A)
2025-06-20 19:55:41 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:54515] (udp) / 'smtp.buap.mx.' (A) / RRs: A
2025-06-20 19:55:46 [DNSHandler:HoneyResolver] Request: [127.0.0.1:50077] (udp) / 'smtp.buap.mx.' (AAAA)
2025-06-20 19:55:46 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:50077] (udp) / 'smtp.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:46 [DNSHandler:HoneyResolver] Request: [127.0.0.1:50078] (udp) / 'smtp.buap.mx.' (CNAME)
2025-06-20 19:55:46 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:50078] (udp) / 'smtp.buap.mx.' (CNAME) / RRs: A


Anaconda Prompt - "C:\ProgramData\miniconda3\condabin\conda.bat" activate ai_security
dns5.buap.mx: ['148.228.1.222']
test.buap.mx: ['148.228.11.42']
www.estudiantes.buap.mx: ['148.228.11.42', 'adminweb.buap.mx.']
viep.buap.mx: ['148.228.11.42']
tituloselectronicos.buap.mx: ['148.228.11.42']
cite.buap.mx: ['148.228.11.42']
conte.buap.mx: ['148.228.8.189']
oral.buap.mx: ['148.228.11.42']
www.bosquedeniebla.buap.mx: ['148.228.11.42']
bosquedeniebla.buap.mx: ['148.228.11.42']
revistanano.buap.mx: ['148.228.11.42']
dapi.buap.mx: ['148.228.11.42']
?>
?>
?>python "14 DNSExploration_EDIT.py"
www.buap.mx: ['10.0.0.0']
mail.buap.mx: ['10.0.0.0']
remote.buap.mx: ['10.0.0.0']
blog.buap.mx: ['10.0.0.0']
webmail.buap.mx: ['10.0.0.0']
server.buap.mx: ['10.0.0.0']
ns.buap.mx: ['10.0.0.0']
smtp.buap.mx: ['10.0.0.0']
pop.buap.mx: ['10.0.0.0']
imap.buap.mx: ['10.0.0.0']
admin.buap.mx: ['10.0.0.0']
secure.buap.mx: ['10.0.0.0']
vpn.buap.mx: ['10.0.0.0']
dns.buap.mx: ['10.0.0.0']
ftp.buap.mx: ['10.0.0.0']
test.buap.mx: ['10.0.0.0']
portal.buap.mx: ['10.0.0.0']
host.buap.mx: ['10.0.0.0']
support.buap.mx: ['10.0.0.0']
dev.buap.mx: ['10.0.0.0']
web.buap.mx: ['10.0.0.0']
mx.buap.mx: ['10.0.0.0']
email.buap.mx: ['10.0.0.0']
cloud.buap.mx: ['10.0.0.0']
owa.buap.mx: ['10.0.0.0']
cdn.buap.mx: ['10.0.0.0']
api.buap.mx: ['10.0.0.0']
exchange.buap.mx: ['10.0.0.0']
mysql.buap.mx: ['10.0.0.0']
wiki.buap.mx: ['10.0.0.0']
cpanel.buap.mx: ['10.0.0.0']
?>

Antes vs después de HoneyResolver:

```
?>nslookup portal.buap.mx
Servidor:  7962v1
Address:  192.168.1.254

*** 7962v1 no encuentra portal.buap.mx: Non-existent domain

?>python "14 DNSExploration_EDIT.py"
www.buap.mx: ['45.60.113.125', 'eskew3g.x.incapdns.net.']
webmail.buap.mx: ['148.228.1.70', 'mx01.siu.buap.mx.']
mx01.siu.buap.mx: ['148.228.1.70']
ns1.buap.mx: ['148.228.1.100']
ns4.buap.mx: ['148.228.1.200']
dns1.buap.mx: ['148.228.1.10']
dns2.buap.mx: ['148.228.153.1']
dns3.buap.mx: ['148.228.203.14']
dns4.buap.mx: ['148.228.1.4']
dns5.buap.mx: ['148.228.1.222']
test.buap.mx: ['148.228.11.42']
www.estudiantes.buap.mx: ['148.228.11.42', 'adminweb.buap.mx.']
viep.buap.mx: ['148.228.11.42']
tituloselectronicos.buap.mx: ['148.228.11.42']
cite.buap.mx: ['148.228.11.42']
conte.buap.mx: ['148.228.8.189']
oral.buap.mx: ['148.228.11.42']
www.bosquedeniebla.buap.mx: ['148.228.11.42']
bosquedeniebla.buap.mx: ['148.228.11.42']
revistanano.buap.mx: ['148.228.11.42']
dapi.buap.mx: ['148.228.11.42']

?>
```

```
?>
?>python "14 DNSExploration_EDIT.py"
www.buap.mx: ['10.0.0.0']
mail.buap.mx: ['10.0.0.0']
remote.buap.mx: ['10.0.0.0']
blog.buap.mx: ['10.0.0.0']
webmail.buap.mx: ['10.0.0.0']
server.buap.mx: ['10.0.0.0']
ns.buap.mx: ['10.0.0.0']
smtp.buap.mx: ['10.0.0.0']
pop.buap.mx: ['10.0.0.0']
imap.buap.mx: ['10.0.0.0']
admin.buap.mx: ['10.0.0.0']
secure.buap.mx: ['10.0.0.0']
vpn.buap.mx: ['10.0.0.0']
dns.buap.mx: ['10.0.0.0']
ftp.buap.mx: ['10.0.0.0']
test.buap.mx: ['10.0.0.0']
portal.buap.mx: ['10.0.0.0']
host.buap.mx: ['10.0.0.0']
support.buap.mx: ['10.0.0.0']
dev.buap.mx: ['10.0.0.0']
web.buap.mx: ['10.0.0.0']
mx.buap.mx: ['10.0.0.0']
email.buap.mx: ['10.0.0.0']
cloud.buap.mx: ['10.0.0.0']
owa.buap.mx: ['10.0.0.0']
cdn.buap.mx: ['10.0.0.0']
api.buap.mx: ['10.0.0.0']
exchange.buap.mx: ['10.0.0.0']
mysql.buap.mx: ['10.0.0.0']
wiki.buap.mx: ['10.0.0.0']
cpanel.buap.mx: ['10.0.0.0']

?>
```

Terminal del defensor pt. 1:

```
Seleccionar Anaconda Prompt - "C:\ProgramData\miniconda3\condabin\conda.bat"  activate ai_security - python  "14 HoneyResolver.py"

?>python "14 HoneyResolver.py"
2025-06-20 19:55:10 [DNSHandler:HoneyResolver] Request: [127.0.0.1:55108] (udp) / 'www.buap.mx.' (A)
2025-06-20 19:55:10 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:55108] (udp) / 'www.buap.mx.' (A) / RRs: A
2025-06-20 19:55:14 [DNSHandler:HoneyResolver] Request: [127.0.0.1:53628] (udp) / 'www.buap.mx.' (AAAA)
2025-06-20 19:55:14 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:53628] (udp) / 'www.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:14 [DNSHandler:HoneyResolver] Request: [127.0.0.1:53629] (udp) / 'www.buap.mx.' (CNAME)
2025-06-20 19:55:14 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:53629] (udp) / 'www.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:14 [DNSHandler:HoneyResolver] Request: [127.0.0.1:53630] (udp) / 'mail.buap.mx.' (A)
2025-06-20 19:55:14 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:53630] (udp) / 'mail.buap.mx.' (A) / RRs: A
2025-06-20 19:55:19 [DNSHandler:HoneyResolver] Request: [127.0.0.1:55373] (udp) / 'mail.buap.mx.' (AAAA)
2025-06-20 19:55:19 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:55373] (udp) / 'mail.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:19 [DNSHandler:HoneyResolver] Request: [127.0.0.1:55374] (udp) / 'mail.buap.mx.' (CNAME)
2025-06-20 19:55:19 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:55374] (udp) / 'mail.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:19 [DNSHandler:HoneyResolver] Request: [127.0.0.1:55375] (udp) / 'remote.buap.mx.' (A)
2025-06-20 19:55:19 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:55375] (udp) / 'remote.buap.mx.' (A) / RRs: A
2025-06-20 19:55:23 [DNSHandler:HoneyResolver] Request: [127.0.0.1:62094] (udp) / 'remote.buap.mx.' (AAAA)
2025-06-20 19:55:23 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:62094] (udp) / 'remote.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:23 [DNSHandler:HoneyResolver] Request: [127.0.0.1:62095] (udp) / 'remote.buap.mx.' (CNAME)
2025-06-20 19:55:23 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:62095] (udp) / 'remote.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:23 [DNSHandler:HoneyResolver] Request: [127.0.0.1:62096] (udp) / 'blog.buap.mx.' (A)
2025-06-20 19:55:23 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:62096] (udp) / 'blog.buap.mx.' (A) / RRs: A
2025-06-20 19:55:28 [DNSHandler:HoneyResolver] Request: [127.0.0.1:59040] (udp) / 'blog.buap.mx.' (AAAA)
2025-06-20 19:55:28 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:59040] (udp) / 'blog.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:28 [DNSHandler:HoneyResolver] Request: [127.0.0.1:59041] (udp) / 'blog.buap.mx.' (CNAME)
2025-06-20 19:55:28 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:59041] (udp) / 'blog.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:28 [DNSHandler:HoneyResolver] Request: [127.0.0.1:59042] (udp) / 'webmail.buap.mx.' (A)
2025-06-20 19:55:28 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:59042] (udp) / 'webmail.buap.mx.' (A) / RRs: A
2025-06-20 19:55:32 [DNSHandler:HoneyResolver] Request: [127.0.0.1:49849] (udp) / 'webmail.buap.mx.' (AAAA)
2025-06-20 19:55:32 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:49849] (udp) / 'webmail.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:32 [DNSHandler:HoneyResolver] Request: [127.0.0.1:49850] (udp) / 'webmail.buap.mx.' (CNAME)
2025-06-20 19:55:32 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:49850] (udp) / 'webmail.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:32 [DNSHandler:HoneyResolver] Request: [127.0.0.1:49851] (udp) / 'server.buap.mx.' (A)
2025-06-20 19:55:32 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:49851] (udp) / 'server.buap.mx.' (A) / RRs: A
2025-06-20 19:55:37 [DNSHandler:HoneyResolver] Request: [127.0.0.1:52665] (udp) / 'server.buap.mx.' (AAAA)
2025-06-20 19:55:37 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:52665] (udp) / 'server.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:37 [DNSHandler:HoneyResolver] Request: [127.0.0.1:52666] (udp) / 'server.buap.mx.' (CNAME)
2025-06-20 19:55:37 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:52666] (udp) / 'server.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:37 [DNSHandler:HoneyResolver] Request: [127.0.0.1:52667] (udp) / 'ns.buap.mx.' (A)
2025-06-20 19:55:37 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:52667] (udp) / 'ns.buap.mx.' (A) / RRs: A
2025-06-20 19:55:41 [DNSHandler:HoneyResolver] Request: [127.0.0.1:54513] (udp) / 'ns.buap.mx.' (AAAA)
2025-06-20 19:55:41 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:54513] (udp) / 'ns.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:41 [DNSHandler:HoneyResolver] Request: [127.0.0.1:54514] (udp) / 'ns.buap.mx.' (CNAME)
2025-06-20 19:55:41 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:54514] (udp) / 'ns.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:41 [DNSHandler:HoneyResolver] Request: [127.0.0.1:54515] (udp) / 'smtp.buap.mx.' (A)
2025-06-20 19:55:41 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:54515] (udp) / 'smtp.buap.mx.' (A) / RRs: A
2025-06-20 19:55:46 [DNSHandler:HoneyResolver] Request: [127.0.0.1:50077] (udp) / 'smtp.buap.mx.' (AAAA)
```

```
2025-06-20 19:55:46 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:50077] (udp) / 'smtp.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:46 [DNSHandler:HoneyResolver] Request: [127.0.0.1:50078] (udp) / 'smtp.buap.mx.' (CNAME)
2025-06-20 19:55:46 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:50078] (udp) / 'smtp.buap.mx.' (CNAME) / RRs: A
```

Terminal del defensor pt. 2:

Seleccionar Anaconda Prompt - "C:\ProgramData\miniconda3\condabin\conda.bat" activate ai_security - python "14 HoneyResolver.py"

```
2025-06-20 19:55:46 [DNSHandler:HoneyResolver] Request: [127.0.0.1:50079] (udp) / 'pop.buap.mx.' (A)
2025-06-20 19:55:46 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:50079] (udp) / 'pop.buap.mx.' (A) / RRs: A
2025-06-20 19:55:50 [DNSHandler:HoneyResolver] Request: [127.0.0.1:58927] (udp) / 'pop.buap.mx.' (AAAA)
2025-06-20 19:55:50 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:58927] (udp) / 'pop.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:50 [DNSHandler:HoneyResolver] Request: [127.0.0.1:58928] (udp) / 'pop.buap.mx.' (CNAME)
2025-06-20 19:55:50 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:58928] (udp) / 'pop.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:50 [DNSHandler:HoneyResolver] Request: [127.0.0.1:58929] (udp) / 'imap.buap.mx.' (A)
2025-06-20 19:55:50 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:58929] (udp) / 'imap.buap.mx.' (A) / RRs: A
2025-06-20 19:55:55 [DNSHandler:HoneyResolver] Request: [127.0.0.1:59703] (udp) / 'imap.buap.mx.' (AAAA)
2025-06-20 19:55:55 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:59703] (udp) / 'imap.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:55 [DNSHandler:HoneyResolver] Request: [127.0.0.1:59704] (udp) / 'imap.buap.mx.' (CNAME)
2025-06-20 19:55:55 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:59704] (udp) / 'imap.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:55 [DNSHandler:HoneyResolver] Request: [127.0.0.1:59705] (udp) / 'admin.buap.mx.' (A)
2025-06-20 19:55:55 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:59705] (udp) / 'admin.buap.mx.' (A) / RRs: A
2025-06-20 19:55:59 [DNSHandler:HoneyResolver] Request: [127.0.0.1:55697] (udp) / 'admin.buap.mx.' (AAAA)
2025-06-20 19:55:59 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:55697] (udp) / 'admin.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:55:59 [DNSHandler:HoneyResolver] Request: [127.0.0.1:55698] (udp) / 'admin.buap.mx.' (CNAME)
2025-06-20 19:55:59 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:55698] (udp) / 'admin.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:55:59 [DNSHandler:HoneyResolver] Request: [127.0.0.1:55699] (udp) / 'secure.buap.mx.' (A)
2025-06-20 19:55:59 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:55699] (udp) / 'secure.buap.mx.' (A) / RRs: A
2025-06-20 19:56:04 [DNSHandler:HoneyResolver] Request: [127.0.0.1:59915] (udp) / 'secure.buap.mx.' (AAAA)
2025-06-20 19:56:04 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:59915] (udp) / 'secure.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:56:04 [DNSHandler:HoneyResolver] Request: [127.0.0.1:59916] (udp) / 'secure.buap.mx.' (CNAME)
2025-06-20 19:56:04 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:59916] (udp) / 'secure.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:56:04 [DNSHandler:HoneyResolver] Request: [127.0.0.1:59917] (udp) / 'vpn.buap.mx.' (A)
2025-06-20 19:56:04 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:59917] (udp) / 'vpn.buap.mx.' (A) / RRs: A
2025-06-20 19:56:08 [DNSHandler:HoneyResolver] Request: [127.0.0.1:54751] (udp) / 'vpn.buap.mx.' (AAAA)
2025-06-20 19:56:08 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:54751] (udp) / 'vpn.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:56:08 [DNSHandler:HoneyResolver] Request: [127.0.0.1:54752] (udp) / 'vpn.buap.mx.' (CNAME)
2025-06-20 19:56:08 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:54752] (udp) / 'vpn.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:56:08 [DNSHandler:HoneyResolver] Request: [127.0.0.1:54753] (udp) / 'dns.buap.mx.' (A)
2025-06-20 19:56:08 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:54753] (udp) / 'dns.buap.mx.' (A) / RRs: A
2025-06-20 19:56:13 [DNSHandler:HoneyResolver] Request: [127.0.0.1:49542] (udp) / 'dns.buap.mx.' (AAAA)
2025-06-20 19:56:13 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:49542] (udp) / 'dns.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:56:13 [DNSHandler:HoneyResolver] Request: [127.0.0.1:49543] (udp) / 'dns.buap.mx.' (CNAME)
2025-06-20 19:56:13 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:49543] (udp) / 'dns.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:56:13 [DNSHandler:HoneyResolver] Request: [127.0.0.1:49544] (udp) / 'ftp.buap.mx.' (A)
2025-06-20 19:56:13 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:49544] (udp) / 'ftp.buap.mx.' (A) / RRs: A
2025-06-20 19:56:17 [DNSHandler:HoneyResolver] Request: [127.0.0.1:51155] (udp) / 'ftp.buap.mx.' (AAAA)
2025-06-20 19:56:17 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:51155] (udp) / 'ftp.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:56:17 [DNSHandler:HoneyResolver] Request: [127.0.0.1:51156] (udp) / 'ftp.buap.mx.' (CNAME)
2025-06-20 19:56:17 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:51156] (udp) / 'ftp.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:56:17 [DNSHandler:HoneyResolver] Request: [127.0.0.1:51157] (udp) / 'test.buap.mx.' (A)
2025-06-20 19:56:17 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:51157] (udp) / 'test.buap.mx.' (A) / RRs: A
```

```
2025-06-20 19:56:22 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:58709] (udp) / 'test.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:56:22 [DNSHandler:HoneyResolver] Request: [127.0.0.1:58710] (udp) / 'portal.buap.mx.' (A)
2025-06-20 19:56:22 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:58710] (udp) / 'portal.buap.mx.' (A) / RRs: A
```

Terminal del defensor pt. 3:

Seleccionar Anaconda Prompt - "C:\ProgramData\miniconda3\condabin\conda.bat" activate ai_security - python "14 HoneyResolver.py"

```
2025-06-20 19:56:27 [DNSHandler:HoneyResolver] Request: [127.0.0.1:53715] (udp) / 'portal.buap.mx.' (AAAA)
2025-06-20 19:56:27 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:53715] (udp) / 'portal.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:56:27 [DNSHandler:HoneyResolver] Request: [127.0.0.1:53716] (udp) / 'portal.buap.mx.' (CNAME)
2025-06-20 19:56:27 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:53716] (udp) / 'portal.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:56:27 [DNSHandler:HoneyResolver] Request: [127.0.0.1:53717] (udp) / 'host.buap.mx.' (A)
2025-06-20 19:56:27 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:53717] (udp) / 'host.buap.mx.' (A) / RRs: A
2025-06-20 19:56:31 [DNSHandler:HoneyResolver] Request: [127.0.0.1:50170] (udp) / 'host.buap.mx.' (AAAA)
2025-06-20 19:56:31 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:50170] (udp) / 'host.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:56:31 [DNSHandler:HoneyResolver] Request: [127.0.0.1:50171] (udp) / 'host.buap.mx.' (CNAME)
2025-06-20 19:56:31 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:50171] (udp) / 'host.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:56:31 [DNSHandler:HoneyResolver] Request: [127.0.0.1:50172] (udp) / 'support.buap.mx.' (A)
2025-06-20 19:56:31 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:50172] (udp) / 'support.buap.mx.' (A) / RRs: A
2025-06-20 19:56:36 [DNSHandler:HoneyResolver] Request: [127.0.0.1:53054] (udp) / 'support.buap.mx.' (AAAA)
2025-06-20 19:56:36 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:53054] (udp) / 'support.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:56:36 [DNSHandler:HoneyResolver] Request: [127.0.0.1:53055] (udp) / 'support.buap.mx.' (CNAME)
2025-06-20 19:56:36 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:53055] (udp) / 'support.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:56:36 [DNSHandler:HoneyResolver] Request: [127.0.0.1:53056] (udp) / 'dev.buap.mx.' (A)
2025-06-20 19:56:36 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:53056] (udp) / 'dev.buap.mx.' (A) / RRs: A
2025-06-20 19:56:40 [DNSHandler:HoneyResolver] Request: [127.0.0.1:56996] (udp) / 'dev.buap.mx.' (AAAA)
2025-06-20 19:56:40 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:56996] (udp) / 'dev.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:56:40 [DNSHandler:HoneyResolver] Request: [127.0.0.1:56997] (udp) / 'dev.buap.mx.' (CNAME)
2025-06-20 19:56:40 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:56997] (udp) / 'dev.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:56:40 [DNSHandler:HoneyResolver] Request: [127.0.0.1:56998] (udp) / 'web.buap.mx.' (A)
2025-06-20 19:56:40 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:56998] (udp) / 'web.buap.mx.' (A) / RRs: A
2025-06-20 19:56:45 [DNSHandler:HoneyResolver] Request: [127.0.0.1:61428] (udp) / 'web.buap.mx.' (AAAA)
2025-06-20 19:56:45 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:61428] (udp) / 'web.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:56:45 [DNSHandler:HoneyResolver] Request: [127.0.0.1:61429] (udp) / 'web.buap.mx.' (CNAME)
2025-06-20 19:56:45 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:61429] (udp) / 'web.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:56:45 [DNSHandler:HoneyResolver] Request: [127.0.0.1:61430] (udp) / 'mx.buap.mx.' (A)
2025-06-20 19:56:45 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:61430] (udp) / 'mx.buap.mx.' (A) / RRs: A
2025-06-20 19:56:49 [DNSHandler:HoneyResolver] Request: [127.0.0.1:63704] (udp) / 'mx.buap.mx.' (AAAA)
2025-06-20 19:56:49 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:63704] (udp) / 'mx.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:56:49 [DNSHandler:HoneyResolver] Request: [127.0.0.1:63705] (udp) / 'mx.buap.mx.' (CNAME)
2025-06-20 19:56:49 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:63705] (udp) / 'mx.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:56:49 [DNSHandler:HoneyResolver] Request: [127.0.0.1:63706] (udp) / 'email.buap.mx.' (A)
2025-06-20 19:56:49 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:63706] (udp) / 'email.buap.mx.' (A) / RRs: A
2025-06-20 19:56:54 [DNSHandler:HoneyResolver] Request: [127.0.0.1:63766] (udp) / 'email.buap.mx.' (AAAA)
2025-06-20 19:56:54 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:63766] (udp) / 'email.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:56:54 [DNSHandler:HoneyResolver] Request: [127.0.0.1:63767] (udp) / 'email.buap.mx.' (CNAME)
2025-06-20 19:56:54 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:63767] (udp) / 'email.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:56:54 [DNSHandler:HoneyResolver] Request: [127.0.0.1:63768] (udp) / 'cloud.buap.mx.' (A)
2025-06-20 19:56:54 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:63768] (udp) / 'cloud.buap.mx.' (A) / RRs: A
2025-06-20 19:56:58 [DNSHandler:HoneyResolver] Request: [127.0.0.1:50070] (udp) / 'cloud.buap.mx.' (AAAA)
```

```
2025-06-20 19:56:58 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:50072] (udp) / 'owa.buap.mx.' (A) / RRs: A
2025-06-20 19:57:03 [DNSHandler:HoneyResolver] Request: [127.0.0.1:50723] (udp) / 'owa.buap.mx.' (AAAA)
2025-06-20 19:57:03 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:50723] (udp) / 'owa.buap.mx.' (AAAA) / RRs: A
```

Terminal del defensor pt. 4:

Seleccionar Anaconda Prompt - "C:\ProgramData\miniconda3\condabin\conda.bat" activate ai_security - python "14 HoneyResolver.py"

```
2025-06-20 19:57:03 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:50723] (udp) / 'owa.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:57:03 [DNSHandler:HoneyResolver] Request: [127.0.0.1:50724] (udp) / 'owa.buap.mx.' (CNAME)
2025-06-20 19:57:03 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:50724] (udp) / 'owa.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:57:03 [DNSHandler:HoneyResolver] Request: [127.0.0.1:50725] (udp) / 'admin.buap.mx.' (A)
2025-06-20 19:57:03 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:50725] (udp) / 'admin.buap.mx.' (A) / RRs: A
2025-06-20 19:57:07 [DNSHandler:HoneyResolver] Request: [127.0.0.1:57435] (udp) / 'admin.buap.mx.' (AAAA)
2025-06-20 19:57:07 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:57435] (udp) / 'admin.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:57:07 [DNSHandler:HoneyResolver] Request: [127.0.0.1:57436] (udp) / 'admin.buap.mx.' (CNAME)
2025-06-20 19:57:07 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:57436] (udp) / 'admin.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:57:07 [DNSHandler:HoneyResolver] Request: [127.0.0.1:57437] (udp) / 'cdn.buap.mx.' (A)
2025-06-20 19:57:07 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:57437] (udp) / 'cdn.buap.mx.' (A) / RRs: A
2025-06-20 19:57:12 [DNSHandler:HoneyResolver] Request: [127.0.0.1:56763] (udp) / 'cdn.buap.mx.' (AAAA)
2025-06-20 19:57:12 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:56763] (udp) / 'cdn.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:57:12 [DNSHandler:HoneyResolver] Request: [127.0.0.1:56764] (udp) / 'cdn.buap.mx.' (CNAME)
2025-06-20 19:57:12 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:56764] (udp) / 'cdn.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:57:12 [DNSHandler:HoneyResolver] Request: [127.0.0.1:56765] (udp) / 'api.buap.mx.' (A)
2025-06-20 19:57:12 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:56765] (udp) / 'api.buap.mx.' (A) / RRs: A
2025-06-20 19:57:16 [DNSHandler:HoneyResolver] Request: [127.0.0.1:61764] (udp) / 'api.buap.mx.' (AAAA)
2025-06-20 19:57:16 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:61764] (udp) / 'api.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:57:16 [DNSHandler:HoneyResolver] Request: [127.0.0.1:61765] (udp) / 'api.buap.mx.' (CNAME)
2025-06-20 19:57:16 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:61765] (udp) / 'api.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:57:16 [DNSHandler:HoneyResolver] Request: [127.0.0.1:61766] (udp) / 'exchange.buap.mx.' (A)
2025-06-20 19:57:16 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:61766] (udp) / 'exchange.buap.mx.' (A) / RRs: A
2025-06-20 19:57:21 [DNSHandler:HoneyResolver] Request: [127.0.0.1:58264] (udp) / 'exchange.buap.mx.' (AAAA)
2025-06-20 19:57:21 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:58264] (udp) / 'exchange.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:57:21 [DNSHandler:HoneyResolver] Request: [127.0.0.1:58265] (udp) / 'exchange.buap.mx.' (CNAME)
2025-06-20 19:57:21 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:58265] (udp) / 'exchange.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:57:21 [DNSHandler:HoneyResolver] Request: [127.0.0.1:58266] (udp) / 'mysql.buap.mx.' (A)
2025-06-20 19:57:21 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:58266] (udp) / 'mysql.buap.mx.' (A) / RRs: A
2025-06-20 19:57:25 [DNSHandler:HoneyResolver] Request: [127.0.0.1:54042] (udp) / 'mysql.buap.mx.' (AAAA)
2025-06-20 19:57:25 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:54042] (udp) / 'mysql.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:57:25 [DNSHandler:HoneyResolver] Request: [127.0.0.1:54043] (udp) / 'mysql.buap.mx.' (CNAME)
2025-06-20 19:57:25 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:54043] (udp) / 'mysql.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:57:25 [DNSHandler:HoneyResolver] Request: [127.0.0.1:54044] (udp) / 'wiki.buap.mx.' (A)
2025-06-20 19:57:25 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:54044] (udp) / 'wiki.buap.mx.' (A) / RRs: A
2025-06-20 19:57:30 [DNSHandler:HoneyResolver] Request: [127.0.0.1:62512] (udp) / 'wiki.buap.mx.' (AAAA)
2025-06-20 19:57:30 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:62512] (udp) / 'wiki.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:57:30 [DNSHandler:HoneyResolver] Request: [127.0.0.1:62513] (udp) / 'wiki.buap.mx.' (CNAME)
2025-06-20 19:57:30 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:62513] (udp) / 'wiki.buap.mx.' (CNAME) / RRs: A
2025-06-20 19:57:30 [DNSHandler:HoneyResolver] Request: [127.0.0.1:62514] (udp) / 'cpanel.buap.mx.' (A)
2025-06-20 19:57:30 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:62514] (udp) / 'cpanel.buap.mx.' (A) / RRs: A
2025-06-20 19:57:34 [DNSHandler:HoneyResolver] Request: [127.0.0.1:61651] (udp) / 'cpanel.buap.mx.' (AAAA)
2025-06-20 19:57:34 [DNSHandler:HoneyResolver] Reply: [127.0.0.1:61651] (udp) / 'cpanel.buap.mx.' (AAAA) / RRs: A
2025-06-20 19:57:34 [DNSHandler:HoneyResolver] Request: [127.0.0.1:61652] (udp) / 'cpanel.buap.mx.' (CNAME)
```