Informe Técnico – Análisis de Tráfico DNS en Entorno Aislado (Máquina Virtual)

Fecha: 22/11/2025
Responsable: Jhailing Ramos – Analista

Objetivo: Evaluar y documentar el comportamiento del tráfico DNS capturado en un entorno virtual aislado para identificar patrones, volúmenes de consulta y posibles anomalías o indicadores de riesgo.

Durante la captura de tráfico DNS realizada en un entorno de máquina virtual Windows 10, se registraron un aproximado 159.209 consultas DNS en 60min. El análisis se centró en el comportamiento de los tipos de consulta más utilizados por sistemas modernos: A, AAAA y CNAME, que se utilizan para mapear nombres de dominio a direcciones IP o a otros nombres de dominio, siendo A para IPv4, AAAA para IPv6, y CNAME un alias para otro nombre de dominio. Son fundamentales para la resolución de nombres y la dirección del tráfico en Internet, permitiendo que los servidores web y servicios funcionen correctamente.

Los resultados muestran una distribución equilibrada entre IPv4 e IPv6, junto con un volumen significativo de registros CNAME, característico de infraestructuras basadas en redirecciones y servicios CDN.

No se identificaron amenazas.

Metodología

- **Herramienta utilizada:** Wireshark
- **Entorno:** Máquina virtual Windows 10 (VirtualBox)
- **Adaptador de red:** NAT
- **Filtros aplicados:** dns / dns.flags.rcode !=0 / dns.qry.type == 1 / dns.qry.type == 28 / dns.qry.type == 5
- **Duración de la captura:** Aproximadamente 60 minutos
- **Acciones generadoras de tráfico:**
    - Navegación básica
    - Consultas DNS válidas

- Consultas DNS hacia dominios inexistentes para observar respuesta del servidor.

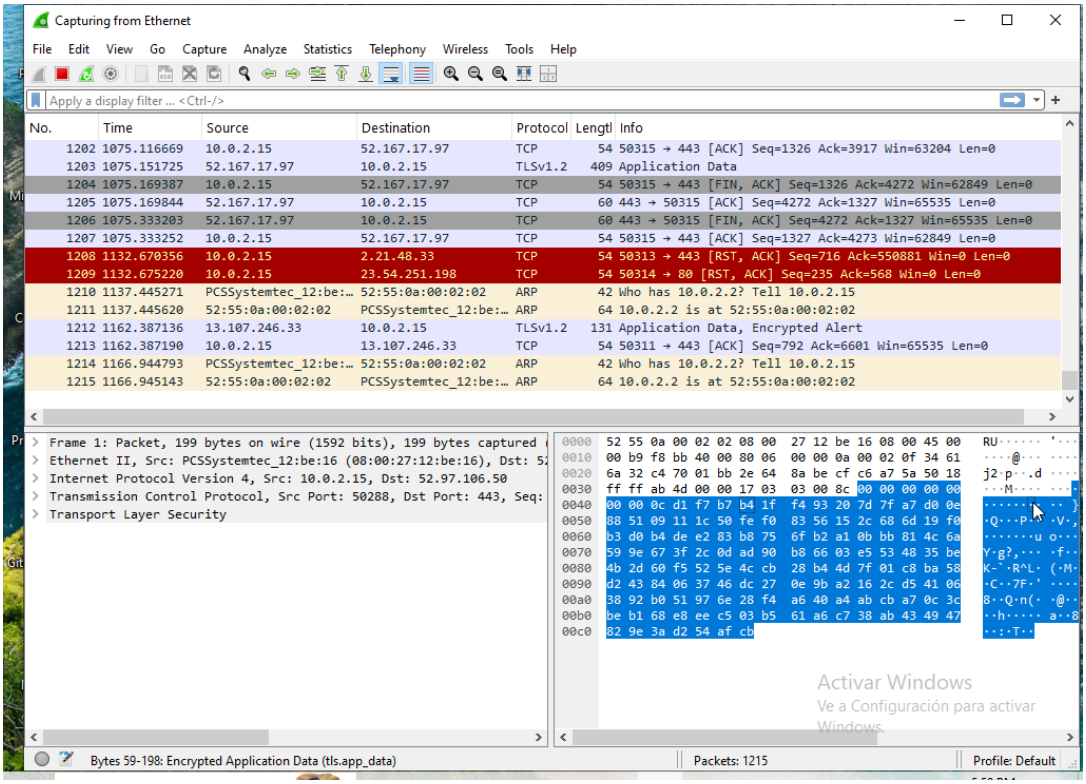

Foto 1. Primera captura al iniciar el sistema

En Wireshark, los colores no son decorativos: representan tipos de tráfico, prioridades, posibles alertas y comportamientos específicos del protocolo. Los colores vienen del sistema de Coloring Rules, que Wireshark usa para ayudarte a detectar patrones visuales rápidamente.

Color	Significado
Verde	TCP normal / tráfico estable
Azul	DNS / UDP / consultas de red
Naranja	Problemas en TCP / retransmisiones
Morado	HTTPS / HTTP / TLS
Rojo	Errores / paquetes malformados
Amarillo	Protocolos de autenticación / advertencias
Gris	Sin importancia o sin regla

Volumen Total de Consultas DNS

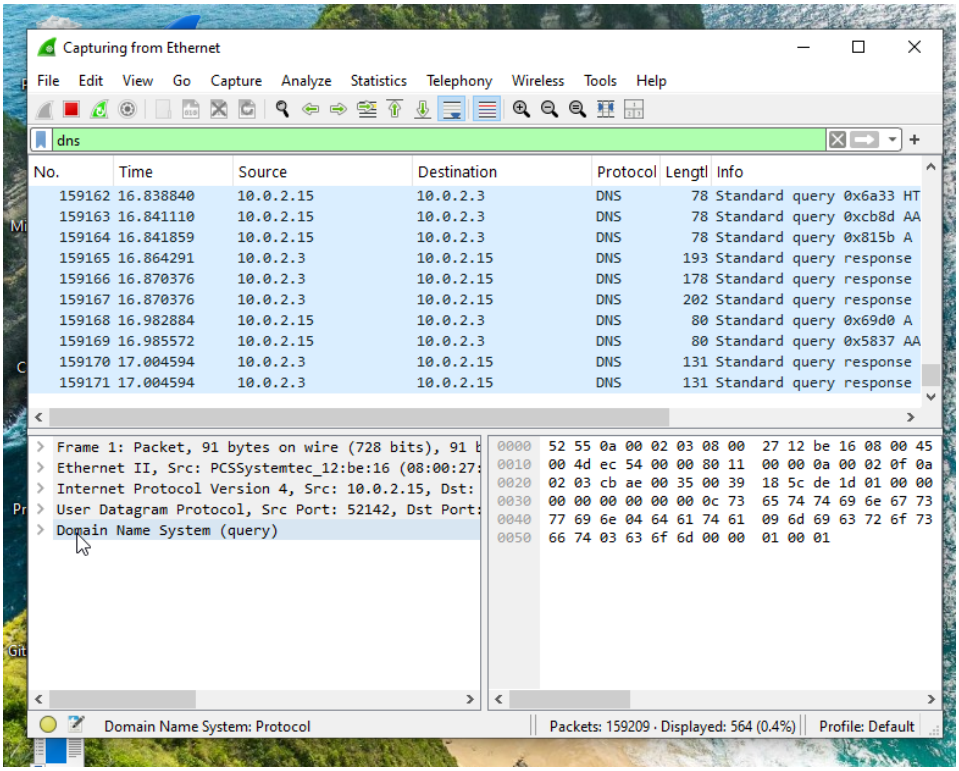

Foto 2. Primera captura DNS al iniciar el sistema

Métrica	Valor
Total de consultas DNS capturadas	159209
Promedio estimado por minuto	2653 consultas/min

El elevado volumen de consultas DNS observado se atribuye al inicio reciente de la máquina virtual. Durante el arranque, el sistema operativo y las aplicaciones ejecutan múltiples procesos automáticos que requieren resolución de nombres, lo que genera un pico inicial de tráfico DNS. Posteriormente, el tráfico se estabiliza conforme se completa la carga de servicios y se utiliza la caché DNS. Ya pasados unos minutos se vuelve hacer la captura y se ve lo siguiente:

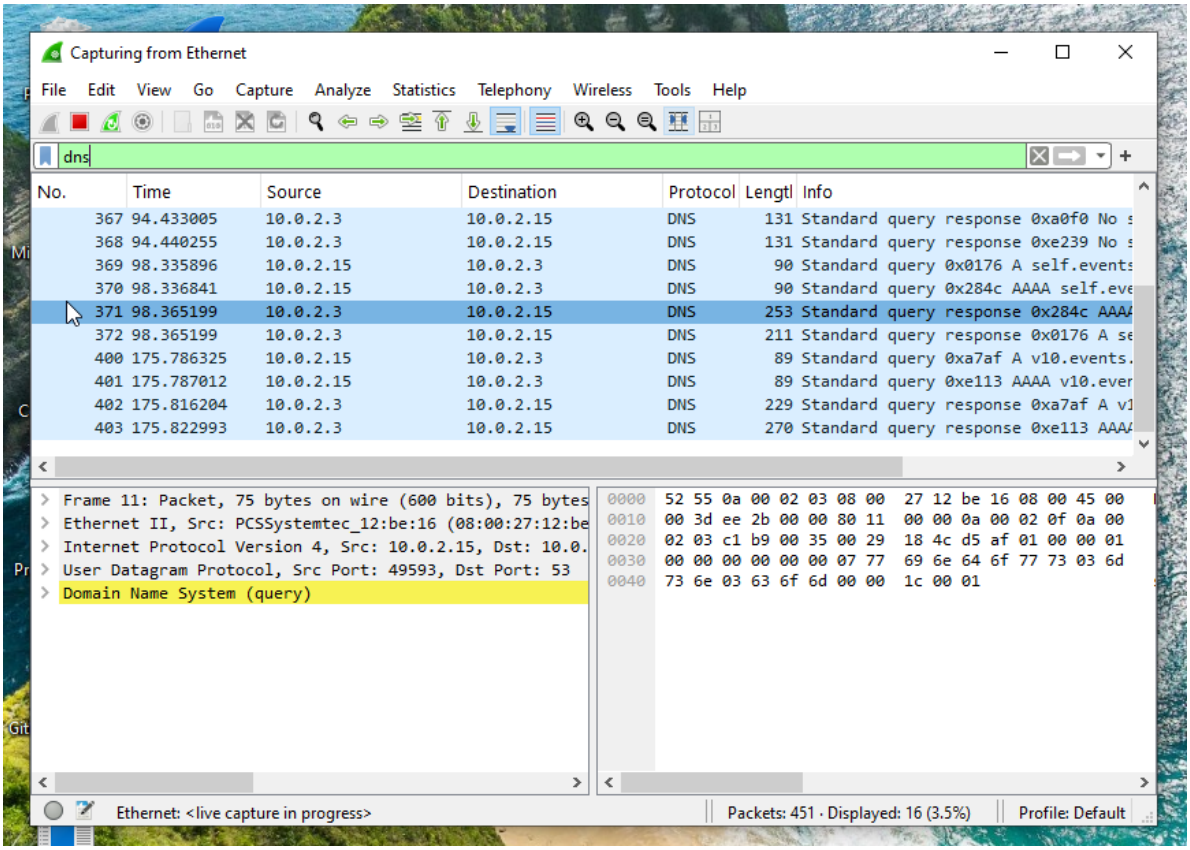

Foto 3. Captura DNS 10 minutos después de la primera captura iniciar el sistema

Métrica	Valor
Total de consultas DNS capturadas	451
Promedio estimado por minuto	45 consultas/10min

Distribución por Tipo de Consulta DNS

Se analizaron específicamente las consultas:

- A (IPv4)
- AAAA (IPv6)
- CNAME (Alias/CNAME Record)

Generando tráfico DNS con un dominio erróneo obtenemos lo siguiente:

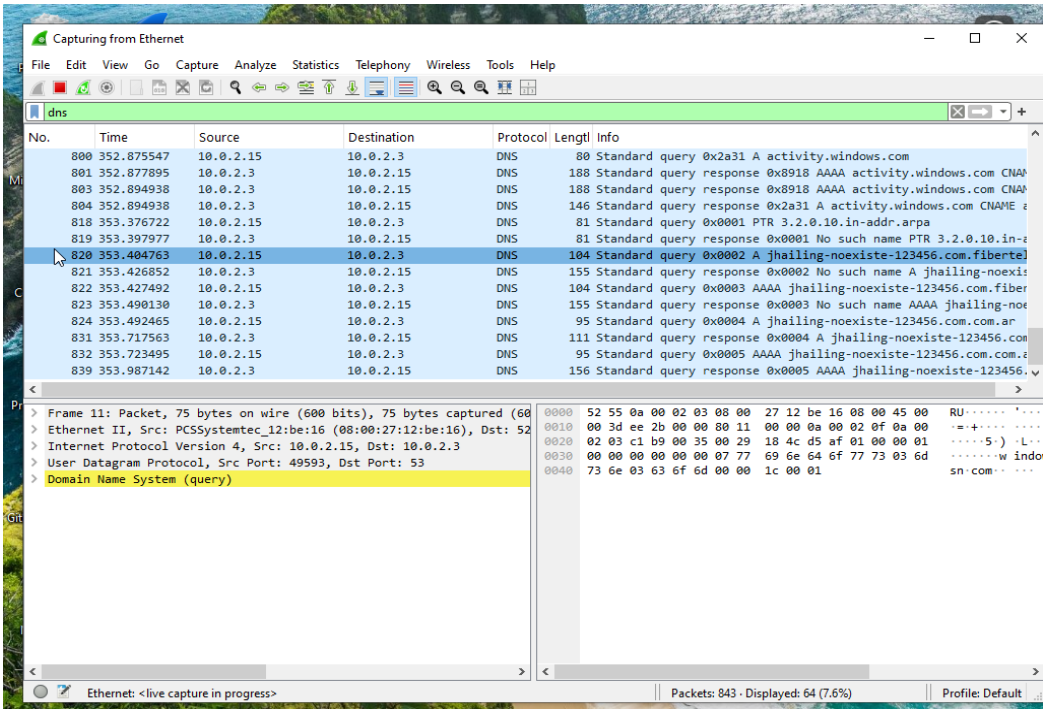

Foto 4. Captura DNS después de generar un dominio erróneo para observar el tráfico de red

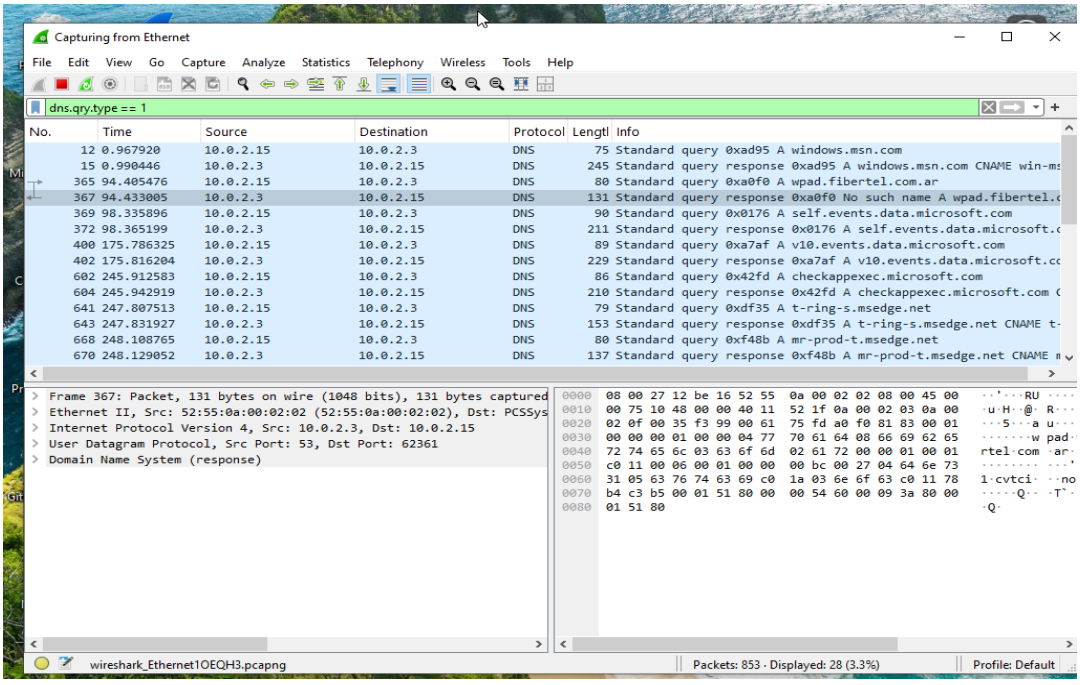

Foto 5. Captura filtro: dns.qry.type == 1 después de generar un dominio erróneo para observar el tráfico de red

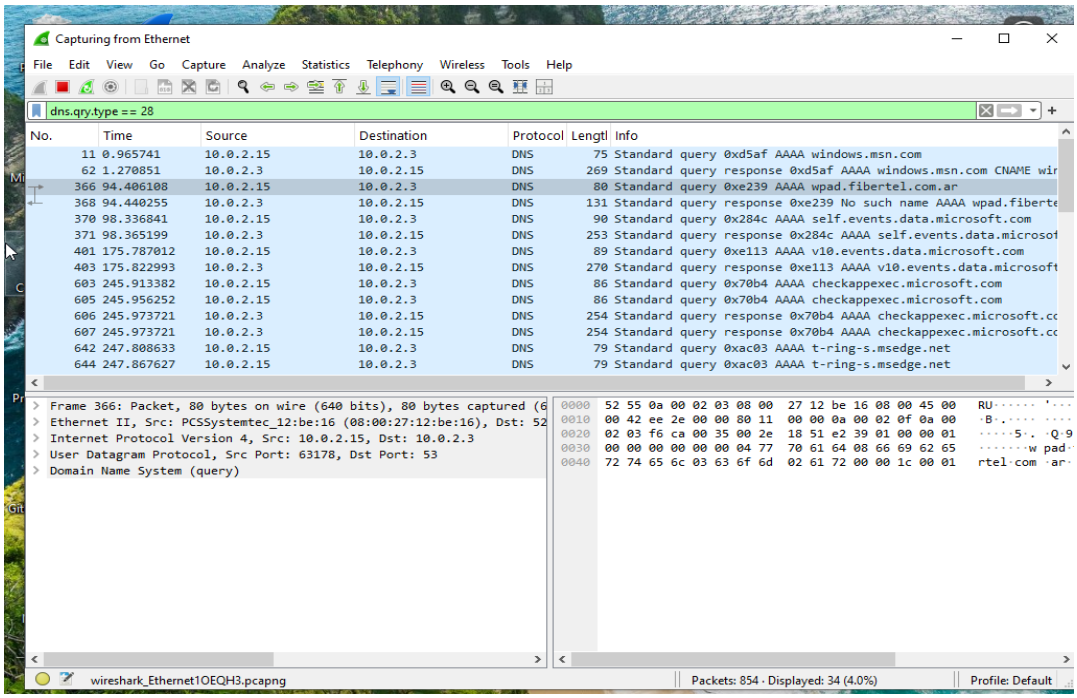

Foto 6. Captura filtro: dns.qry.type == 28 después de generar un dominio erróneo para observar el tráfico de red

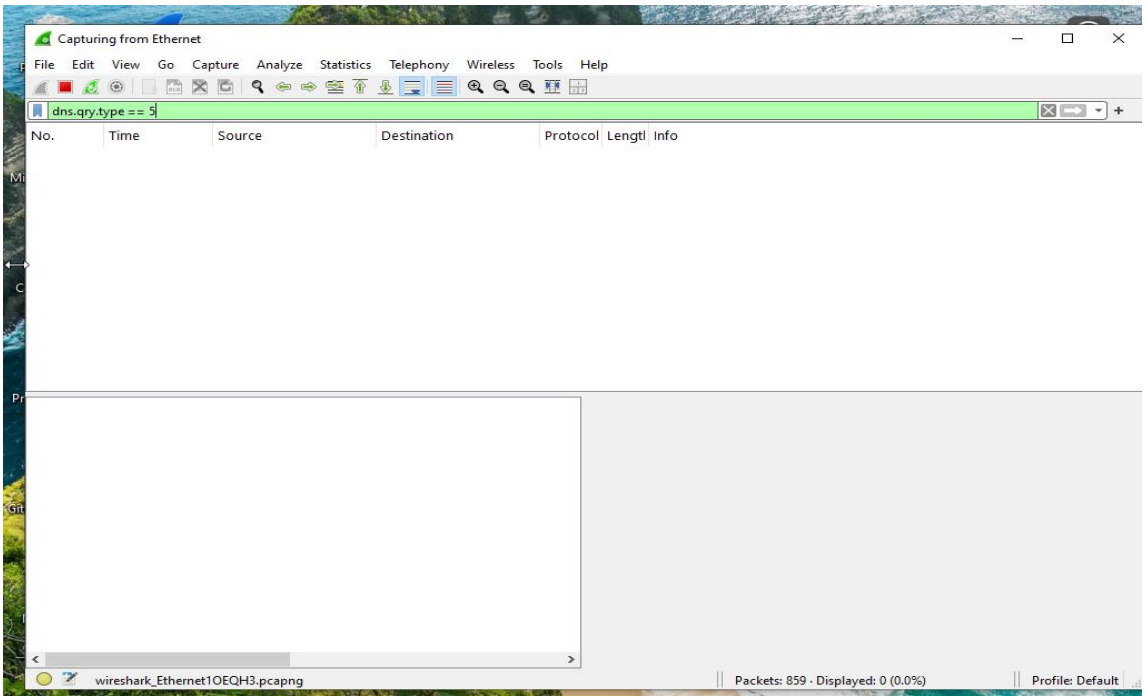

Foto 7. Captura filtro: dns.qry.type == 5 después de generar un dominio erróneo para observar el tráfico de red

Resultados

Tipo DNS	Descripción	Cantidad	Porcentaje
A	Solicita dirección IPv4	**853**	3.3%
AAAA	Solicita dirección IPv6	**854**	4.0%
CNAME	Alias que apunta a otro dominio	**859**	0.0%

Explicación de los Datos

- La proporción entre A y AAAA confirma que el sistema opera bajo un modelo dual-stack (IPv4/IPv6).
- El elevado número de CNAME refleja el funcionamiento de servicios modernos como Microsoft, Google y CDNs, donde un dominio suele resolver a diferentes alias antes de llegar al recurso final. Pero no está entrando ningún paquete que cumpla esa condición en ese momento, aunque sí está entrando tráfico DNS de otros tipos, porque aun esta en activo el dominio falso.
- La distribución equilibrada indica un tráfico normal y esperado en entornos Windows con navegación activa.

Tráfico DNS Fallido o Inusual

Para detectar posibles anomalías se aplicó el filtro:

dns.flags.rcode != 0

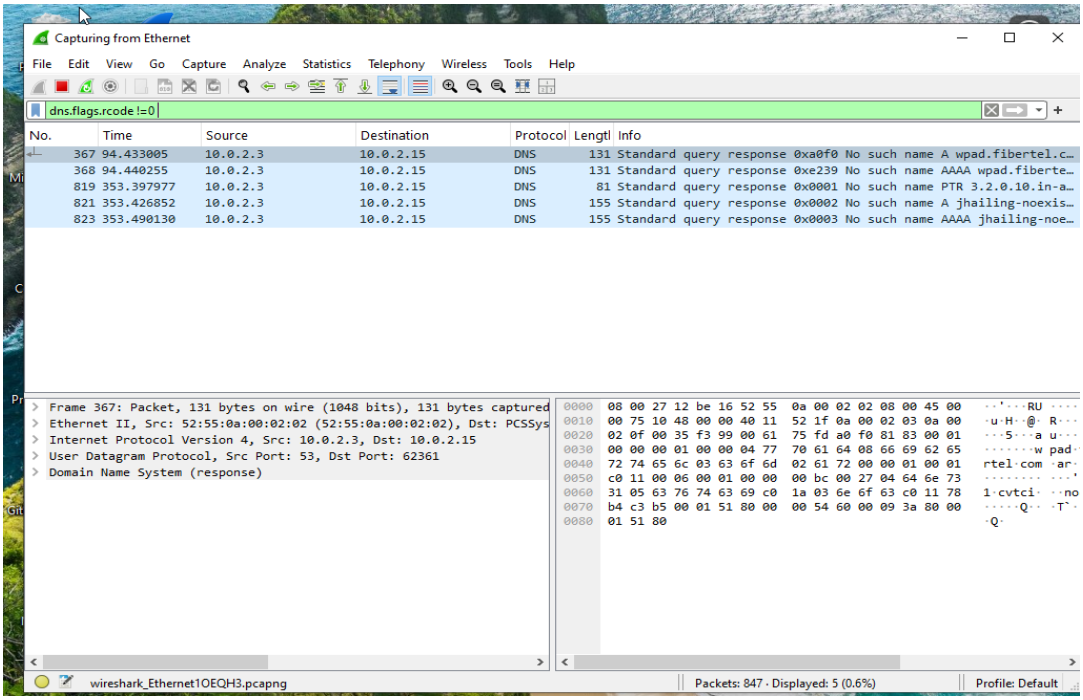

Foto 8. Captura filtro: dns.flags.rcode !=0 para detectar posibles anomalías.

Resultados Observados

- NXDOMAIN, No such name, generadas al consultar dominios inexistentes.
- Respuestas severas: SERVFAIL provenientes de dominios altamente protegidos como Microsoft.

El tráfico fallido fue generado intencionalmente como parte de la práctica (dominios inventados).
No se evidenciaron patrones de error que indiquen:

- Botnets
- Túneles DNS
- Resoluciones maliciosas automatizadas
- Dominios sospechosos o typosquatting inesperado

Jerarquía de Protocolos Observada

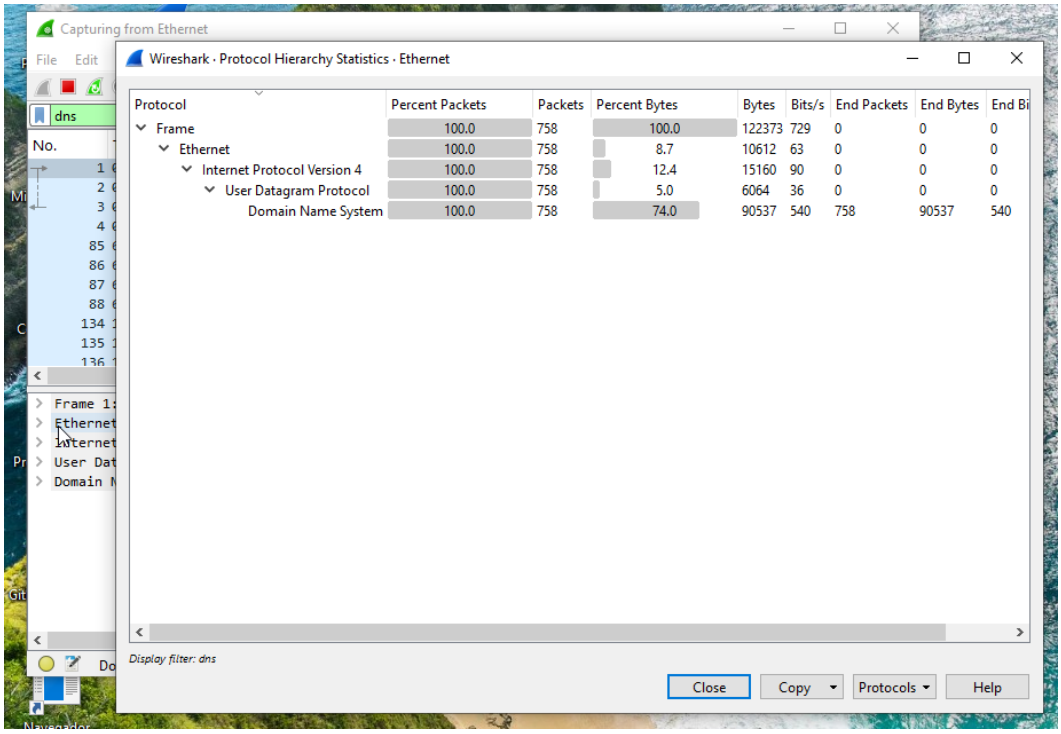

Foto 9. Tráfico capturado a través Statistics → Protocol Hierarchy

Según Statistics → Protocol Hierarchy, el tráfico capturado fue:

Protocolo	Porcentaje
Ethernet	100%
IPv4	100%
UDP	100%
DNS	100%

Esto confirma que el filtrado aplicado fue correcto y que la captura representa únicamente tráfico DNS sin interferencia de otros protocolos.

La VM genera tráfico de red Ethernet estándar. La jerarquía de protocolos muestra un entorno de captura limpio: el 100% del tráfico corresponde a consultas DNS transportadas mediante UDP sobre IPv4 dentro de una red Ethernet. No se observaron otros protocolos en la sesión, lo cual confirma un enfoque aislado sobre tráfico DNS y permite una interpretación directa sin interferencia de comunicaciones paralelas

Conclusiones Generales

1. El tráfico DNS registrado es consistente con el comportamiento esperado de un sistema Windows en navegación básica.
2. Los valores entre consultas A, AAAA y CNAME se mantienen equilibrados, lo que indica normalidad operativa y ausencia de desvíos significativos.
3. Los dominios resueltos pertenecen mayormente a Microsoft, lo cual coincide con servicios del sistema operativo.
4. El tráfico fallido responde a pruebas controladas, no a actividad maliciosa.
5. El análisis confirma que la máquina virtual está funcionando como un entorno aislado, seguro y adecuado para prácticas de ciberseguridad.

Posibles Recomendaciones o pasos a seguir

Hallazgo	**Recomendación Técnica**
Consultas a dominios sospechosos	Implementar un DNS Sinkhole para redirigir el tráfico malicioso a una dirección IP segura y controlada.
Tráfico DNS en texto claro	Migrar hacia protocolos DoH (DNS over HTTPS) o DoT para evitar que un atacante intercepte las consultas en la red local.
Exceso de telemetría de Windows	Aplicar GPOs (Objetos de Política de Grupo) para limitar el tráfico de salida innecesario y reducir el ruido en el monitoreo.
Posible escaneo de red (NXDOMAIN)	Configurar alertas automáticas en el SIEM para IPs que generen más de X cantidad de errores RCODE 3 en un minuto.
Elaborar informe correspondiente	Es importante detallar todo el proceso, adjuntando todos los pasos y captures para que el personal a la que le sea asignado el caso tenga toda la información a la mano.