www.eysglobal.com

CURSO DE INFORMÁTICA FORENSE

MÓDULO 3

Tecnologías y protocolos

Protocolos comunes de monitoreo

Syslog y NTP

DNS

- Actualmente, muchos tipos de malware usan el DNS. Algunas variantes de malware emplean el DNS para comunicarse con servidores de comando y control (CnC) y para exfiltrar datos de tráfico disfrazados de consultas de DNS normales.
- El malware podría codificar datos robados como una parte del subdominio de una búsqueda de DNS en un dominio donde el servidor de nombres esté bajo control de un atacante.

Protocolos de Correo Electrónico

Tecnologías de seguridad

ACL NAT y PAT

Conexión de red peer-to-peer y Tor

Trabajo con datos de seguridad de la red

Investigación de datos de la red

Uso de Sguil

Consultas de Sguil

Alternar a otros programas desde Sguil

Uso de ELK

¿Cómo mejorar el trabajo del analista de ciberseguridad?

Análisis y respuesta de incidentes e informática forense digital

Manejo de evidencia y atribución del ataque

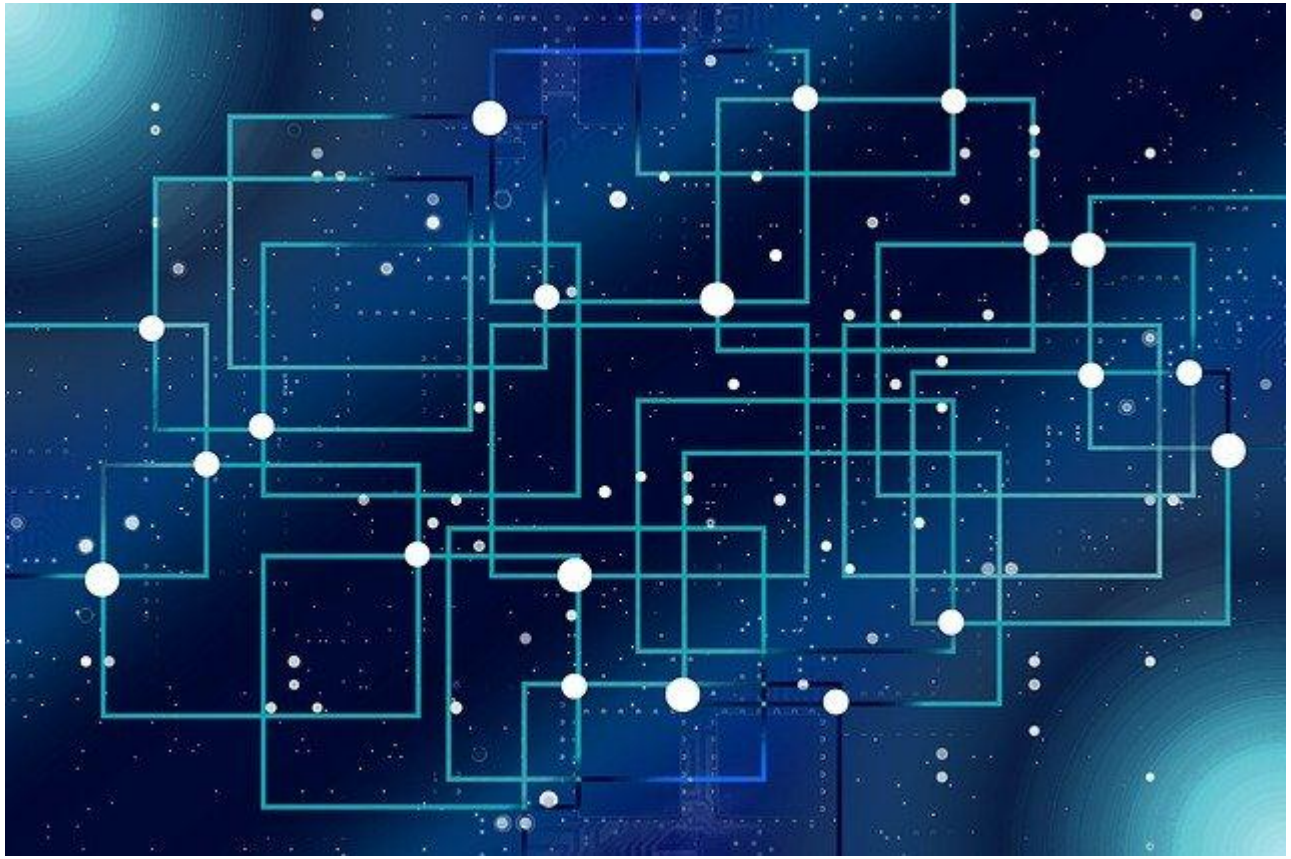
INFORMÁTICA FORENSE

El proceso de informática forense digital

- **Recopilación**- la identificación de posibles fuentes de datos forenses y la obtención, el manejo y el almacenamiento de esos datos.
- **Examen** - evaluar y extraer información relevante de los datos recopilados**.**
- **Análisis** - Extraer conclusiones a partir de los datos y la correlación de datos de múltiples fuentes
- **Informes** - Preparación y presentación de información resultante de la fase de análisis.

INFORMÁTICA FORENSE

Integridad y preservación de los datos



Cadenas de Eliminación Cibernética

Análisis del modelo de diamante de las intrusiones

Respuesta ante incidentes

- ¿Cómo establecer una capacidad de respuesta ante los incidentes?

Ciclo útil de la respuesta ante los incidentes de NIST

Requisitos para la creación de informes y el intercambio de información