CURSO PESQUISA EM FONTES ABERTAS – TÉCNICAS E FERRAMENTAS
TURMA 2

Data: 24, 25 e 26 de setembro de 2024

Local: CEAF

CONTEÚDO PROGRAMÁTICO

Instrutoras:

Adriana Shimabukuro | Chefe do Núcleo Técnico de Combate aos Crimes Cibernéticos da Procuradoria da República /SP – MPF

Renata Galvão de Medeiros Polizer | Analista da Procuradoria da República /SP – MPF

A) Introdução a pesquisa cibernética:
Motivação de criminosos, Perfis, Modus Operandi, Assinatura e Principais linhas de investigação.

B) Pesquisa de sites
Conceitos de IP, sites, porta lógica, diferença entre registrante e localização do site, sites com proteção à privacidade (bulletproof hosting), bloqueios de sites, ferramentas: whois, dnshistory, wayback machine e casos práticos.

C) Pesquisa em e-mails
Conceitos: cabeçalhos de email, criptografia e o uso do e-mail isca.
Casos* práticos*: uso do e-mail para capturar geolocalização do alvo.

D) Pesquisa nas redes sociais
Como localizar nomes, e-mails, telefones nas redes sociais, principais ferramentas para cruzamento de perfis, buscas de trends topics e fake news. Como acionar os provedores (facebook, instagram etc) e ferramentas para coletas de dados.

E) Pesquisa telefonia fixa e celulares
Diferença entre interceptação telemática tradicional e a interceptação telemática nas pontas. Geolocalização. Spywares comerciais. Configuração de celulares investigativos.

F) Análise de imagens e vídeos
Conceitos de metadados, ferramentas de análises e casos práticos.

G) Pesquisa dos mensageiros Instantâneos (Whatsapp, Telegram, etc.)
Conceitos de criptografia, funcionamento da criptografia ponto a ponto, interceptação no Whatsapp, acesso a dados de nuvem. Investigação no Telegram.

H) IoT – Internet das coisas
Cibersegurança, ferramenta Shodan e principais expressões utilizadas para a busca de equipamentos abertos na Internet.

I) Configuração do ambiente de pesquisa
Instalação e configuração de máquina virtual (OracleVM) e principais distribuições LINUX para investigadores.

J) Pesquisa na DarkNet e criptomoedas
Conceitos: Diferença entre DeepWeb e DarkNet, tecnologia TOR, ferramentas para rastreamento de moedas virtuais e blockchain. Mercados de venda de drogas e equipamentos ilícitos na darkweb.

K) Cadeia de Custódia
Conceitos, hash, tipos de coleta, softwares/equipamentos.

CEAF
Centro de Estudos e Aperfeiçoamento Funcional

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA