BAB I
PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi digital telah membawa perubahan signifikan dalam komunikasi global, khususnya melalui media email. Email menjadi salah satu sarana komunikasi utama dalam berbagai sektor, mulai dari pendidikan, bisnis, hingga pemerintahan. Namun, kemudahan ini tidak lepas dari potensi ancaman keamanan. Menurut laporan dari Kaspersky (2023), "email masih menjadi vektor utama penyebaran serangan siber yang paling berbahaya dan efektif, seperti phishing dan spoofing." Kondisi ini menandakan bahwa meskipun teknologi terus berkembang, kesadaran dan perlindungan terhadap keamanan informasi masih menjadi tantangan besar.

Kedua serangan tersebut merupakan serangan yang saling melengkapi. Para penyerang dalam kategori ini biasanya tertarik pada informasi yang bersifat rahasia yang dimiliki oleh korban. Email spoofing sendiri merupakan teknik manipulasi header email sehingga penerima mengira email tersebut berasal dari sumber yang terpercaya, padahal sebenarnya berasal dari pihak yang tidak berwenang. Di sisi lain, phishing adalah metode yang menggunakan email palsu atau situs web tiruan untuk menipu korban agar memberikan informasi sensitif seperti username, password, dan data keuangan.

Kombinasi teknik spoofing dan phishing dapat menimbulkan risiko keamanan yang sangat besar, baik bagi individu maupun organisasi, karena dapat mengakibatkan pencurian identitas dan kerugian finansial yang signifikan. Lonjakan serangan email palsu dan phishing menjadi ancaman yang signifikan bagi jutaan pengguna internet. Hal ini terus menjadi ancaman bagi individu, organisasi, dan bahkan negara-negara yang menjadi

target. peningkatan aktivitas phishing sebesar 61% pada tahun 2022, melampaui angka yang tercatat pada tahun 2021. Menurut statistik yang dirilis oleh Anti-Phishing Working Group (APWG), terdapat lebih dari 1.270.883 serangan phishing pada kuartal ke-3 tahun 2022, menjadikannya yang terburuk yang pernah tercatat dalam sejarah grup tersebut. Dalam laporan yang sama, 97% korban pelanggaran data dilaporkan setiap jam di seluruh dunia, dengan individu kehilangan rata-rata $136 dalam serangan phishing. (Adewumi & Ani, 2025)

Untuk mengatasi ancaman ini, dibutuhkan analisis forensik digital yang mampu mengidentifikasi, mengumpulkan, dan menganalisis bukti digital pada memori sistem korban. Metode live fornsik menjadi salah satu pendekatan yang bisa dilakukan dalam melakukan investigasi terhadap email spoofing dan phishing karena dapat mengamati keadaan sistem secara mendalam tanpa mengubah data asli. Melalui analisis memori forensik, dapat diungkap pola serangan, teknik yang dipakai pelaku, serta jejak digital yang ditinggalkan yang sangat berguna dalam proses pemulihan dan pencegahan serangan lebih lanjut.

Studi mengenai analisis memori forensik dalam konteks email spoofing dan phishing masih menjadi bidang yang perlu dikembangkan dan diperdalam, terlebih dengan meningkatnya serangan siber yang semakin canggih dan kompleks. Penelitian yang fokus pada pendekatan metode *live fornesic* diharapkan dapat memberikan kontribusi signifikan untuk meningkatkan efektivitas deteksi dan penanganan serangan ini, sehingga keamanan data dan komunikasi pengguna dapat lebih terjaga.

Untuk mencapai tujuan tersebut, penelitian ini akan memanfaatkan metode *live memory forensics* sebagai teknik utama untuk mengumpulkan dan menganalisis bukti digital. Dalam konteks ini, memori sistem (RAM) berfungsi sebagai sumber data krusial yang mencatat setiap aktivitas sistem secara *real-time*, termasuk informasi tentang proses yang sedang berjalan,

koneksi jaringan, dan potensi malware atau injeksi kode yang berhubungan dengan serangan spoofing atau phishing. Dengan menganalisis dump*memori yang diambil saat sistem diduga sedang diserang, peneliti dapat mengidentifikasi artefak, sehingga memungkinkan pengungkapan pola dan karakteristik serangan dengan detail yang lebih mendalam.

B. Rumusan Masalah

1. Bagaimana proses identifikasi artefak digital dalam memori komputer yang berkaitan dengan aktivitas email spoofing dan phishing?
2. Apa saja bukti digital yang dapat ditemukan dalam dump memori (RAM) yang menunjukkan adanya aktivitas phishing dan spoofing?

C. Batasan Masalah

1. Analisis artefak digital dibatasi pada data yang diekstrak dari salinan memori fisik (memory dump atau RAM dump) dari komputer korban. Penelitian tidak mencakup analisis data dari media penyimpanan jangka panjang (seperti hard disk drive atau solid-state drive), log sistem operasi, atau log jaringan eksternal.
2. Identifikasi artefak dan bukti digital hanya difokuskan pada jejak yang ditinggalkan oleh proses runtime (yang sedang berjalan) pada memori, yang berkaitan langsung dengan dua aktivitas spesifik yaitu email spoofing dan phishing.

D. Manfaat Penelitian

1. Memberikan wawasan tentang efektivitas dan kendala tools forensik dalam melakukan akuisisi dan analisis memori.
2. Memberikan Bukti Valid bahwa Memori Volatil Menyimpan Artefak Penting. Temuan dalam penelitian ini menunjukkan bahwa artefak phishing seperti file HTML, input korban, dan aktivitas jaringan tetap terekam di RAM.

3. Penelitian ini membantu menjelaskan secara teknis bagaimana email spoofing dan phishing dilakukan, serta bagaimana serangan ini dapat meninggalkan jejak digital di memori sistem.

E. Tujuan Penelitian

1. Mengidentifikasi proses, file, dan aktivitas jaringan yang berkaitan dengan serangan phishing.
2. Menganalisis email spoofing yang digunakan.
3. Menemukan jejak aktivitas korban.