BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat ditarik kesimpulan sebagai berikut:

1. Implementasi algoritma SVM dan KNN sebagai solusi alternatif terhadap keterbatasan *signature-based detection* yang tidak efektif menghadapi *obfuscated malware* telah berhasil dilakukan menggunakan fitur-fitur analisis forensik memori dari dataset ObfuscatedMalMem2022 dan MalwareMemoryDump. Tahap *preprocessing* yang ketat, khususnya normalisasi menggunakan *Standard Scaler*, terbukti krusial karena kedua algoritma sangat sensitif terhadap perbedaan skala fitur numerik. SVM diimplementasikan secara optimal dengan kernel RBF (C=1.0), sementara KNN mencapai performa terbaik pada nilai K=5 dengan pembobotan berbasis jarak. Pendekatan berbasis analisis memori volatilitas ini terbukti mampu menangkap perilaku *runtime* malware yang tidak dapat dideteksi melalui analisis file statis.
2. Pengukuran efektivitas kedua algoritma dalam mendeteksi pola anomali *obfuscated malware* pada data forensik memori berdimensi tinggi menunjukkan bahwa SVM secara konsisten unggul pada seluruh metrik evaluasi. Pada dataset ObfuscatedMalMem2022, SVM mencapai akurasi 98,87%, *recall* 98,46%, *precision* 97,30%, dan *F1-Score* 97,88%; sedangkan KNN memperoleh akurasi 96,02%, *recall* 96,66%, *precision* 95,45%, dan *F1-Score* 96,05%. Keunggulan SVM terutama terlihat pada minimalisasi *False Negative* (hanya 45 dibanding 98 pada KNN), yang merupakan metrik paling kritis dalam konteks keamanan siber karena berkaitan langsung dengan jumlah malware yang lolos dari deteksi.
3. Penentuan algoritma dengan keseimbangan terbaik antara akurasi deteksi dan efisiensi waktu komputasi menunjukkan hasil yang bergantung pada skenario penggunaan. SVM unggul dari segi akurasi sekaligus kecepatan deteksi (*testing time* 3,21 detik; ~0,55ms per sampel), menjadikannya lebih

layak untuk sistem deteksi *real-time* dengan trafik tinggi. KNN sebaliknya unggul dalam waktu pelatihan (2,15 detik; 21,2x lebih cepat dari SVM 45,67 detik), namun memiliki kelemahan pada *testing time* yang 3,9x lebih lambat akibat keharusan menghitung jarak ke seluruh 23.432 *training samples* untuk setiap prediksi. Dengan mempertimbangkan seluruh aspek *trade-off* ini, SVM direkomendasikan sebagai algoritma terbaik untuk kasus deteksi *obfuscated malware* berbasis forensik memori, khususnya untuk sistem yang memprioritaskan akurasi dan kecepatan respons.

4. Analisis konsistensi performa kedua algoritma pada dua dataset berbeda menunjukkan bahwa SVM mempertahankan keunggulannya secara lintas dataset dengan degradasi akurasi yang terkendali (98,87% ke 96,13% pada MalwareMemoryDump, penurunan <3%), mengindikasikan kemampuan generalisasi yang baik. KNN juga menunjukkan pola serupa namun dengan gap performa lebih besar terhadap SVM pada kedua dataset. Konsistensi ini memvalidasi bahwa rekomendasi algoritma yang dihasilkan tidak hanya berlaku pada satu kondisi data tertentu, melainkan dapat diandalkan sebagai solusi yang robust dalam menghadapi variasi ancaman *obfuscated malware* yang terus berkembang.

5.2 Saran

5.2.1 Saran untuk Penelitian Lanjutan

1. **Prioritas Tinggi (0-6 bulan)**: Melakukan pengujian klasifikasi *multi-class* untuk mengidentifikasi famili malware secara spesifik (misal: membedakan Ransomware dan Spyware).
2. **Prioritas Medium (6-12 bulan)**: Mengeksplorasi penggunaan algoritma *Deep Learning* seperti *Recurrent Neural Networks* (RNN) untuk melihat kemampuannya menangani fitur temporal.
3. **Prioritas Rendah (>12 bulan)**: Mengimplementasikan model dalam sistem *real-time stream* menggunakan trafik memori asli dari jaringan operasional.

5.2.2 Saran untuk Implementasi Praktis

1. **SOC dan Security Teams**: Direkomendasikan menggunakan SVM sebagai mesin deteksi utama karena tingkat *Recall* yang tinggi (98%) guna meminimalkan risiko kebocoran data.

2. **Enterprise IT Departments**: Memasukkan analisis memori volatilitas ke dalam prosedur rutin *Incident Response* untuk mendeteksi ancaman persisten yang tidak memiliki jejak file statis.
3. **Endpoint Protection Vendors**: Mempertimbangkan integrasi model klasifikasi ringan berbasis RAM ke dalam agen EDR (*Endpoint Detection and Response*) guna menghadapi teknik *code packing* terbaru.

5.2.3 Saran untuk Stakeholders Lain

1. **Akademisi dan Researcher**: Memperluas penelitian pada teknik *anti-forensics* yang sengaja memanipulasi artefak memori untuk mengelabuhi model pembelajaran mesin.
2. **Policy Makers dan Regulator**: Mendorong standarisasi penggunaan analisis forensik digital pada infrastruktur kritis nasional.
3. **Malware Dataset Providers**: Menyediakan dataset yang lebih variatif dengan menyertakan lebih banyak sampel malware Linux dan MacOS untuk melengkapi dominasi dataset Windows.

5.3 Penutup

Penelitian ini menegaskan bahwa deteksi malware bukan lagi sekadar mencari tanda tangan file statis, melainkan memahami perilaku dinamis program di dalam memori sistem. Dengan akurasi yang mencapai hampir 99%, penerapan *Machine Learning* pada forensik memori bukan lagi sekadar opsi, melainkan kebutuhan esensial dalam ekosistem pertahanan siber modern untuk melindungi integritas dan kerahasiaan data dari ancaman yang kian canggih.