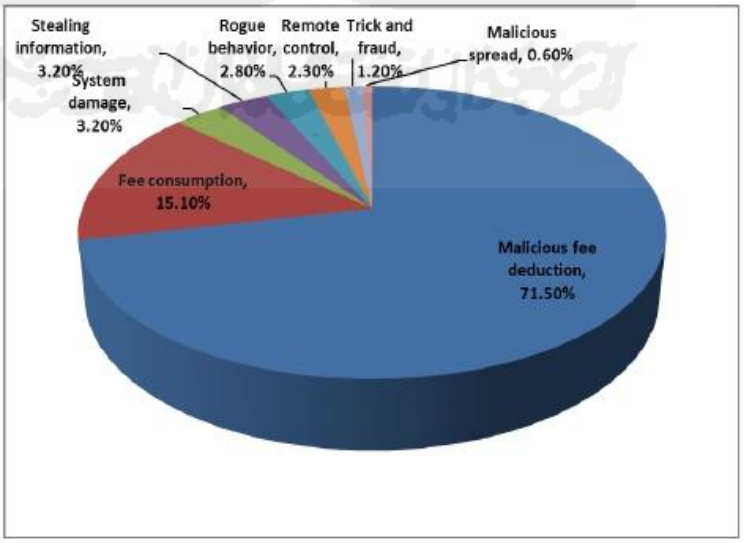
Bab 1 Pendahuluan

1.1 Latar Belakang Penelitian

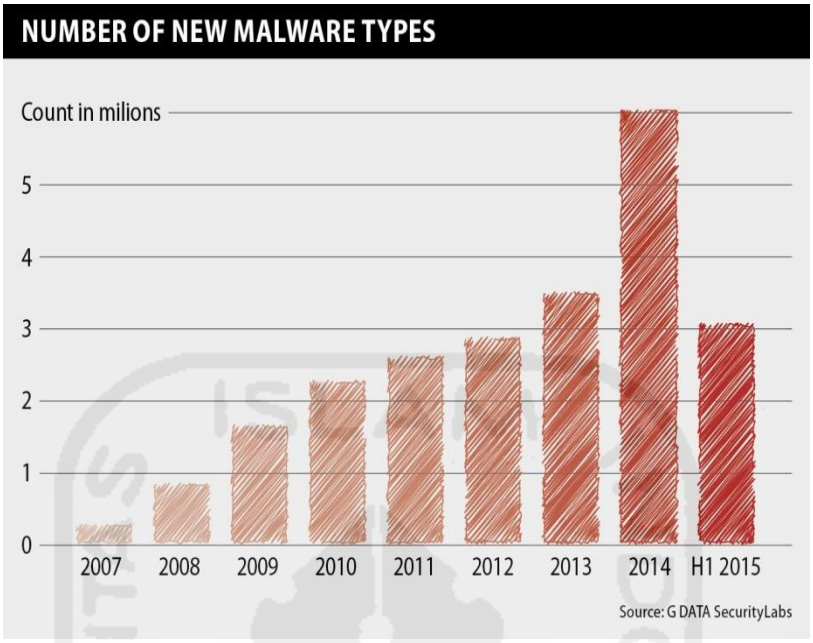
Analisis perangkat lunak berbahaya atau *malware* menjadi salah satu bagian penting dalam bidang forensik digital (Masood, 2004). Kemampuan untuk menganalisa perangkat lunak berbahaya bagi *investigator* menjadi tuntutan dalam setiap melakukan investigasi. Hal ini dikarenakan meningkatnya jumlah *malware* serta evolusi dan mampu beradaptasinya terhadap perangkat analisis yang selama ini digunakan. Analisis *malware* membutuhkan keterampilan khusus untuk melakukan pendeteksian dan memahami cara kerja dari *malware* tersebut, secara garis besar *malware* dibagi atas beberapa kategori yaitu, *worm, virus, trojan horse, adware,* dan *exploit,* penggunaan lima jenis *malware* tersebut merupakan jenis *malware* yang paling sering ditemukan pada analisis *malware* umumnya, yang dimana setiap kategori *malware* mempunyai spesifikasi atau cara kerja yang berbeda (Valli and Brand 2008).

Perkembangan *malware* yang meningkat drastis mendapatkan perhatian khusus dari komunitas dan para peneliti *malware.* Hal ini diperkuat oleh data yang dirilis oleh *National Computer Network Emergency Response Technical Team / Coordination Center of China* terdapat 702,861 contoh program *mobile internet* berbahaya atau *malware* pada tahun 2013, 99,5 persen diantaranya ber-*platform android.*



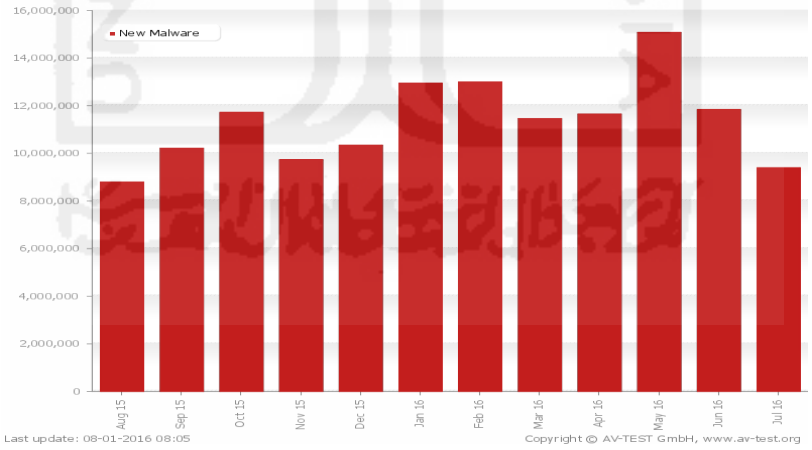
Gambar 1.1 *Mobile Malware Category* 2013

Menurut data yang dirilis oleh *G Data Security Labs* pada tahun 2015, terdapat 3,045,722 varian *malware* baru. Program-program berbahaya ini memiliki ancaman keamanan yang dapat berdampak pada kerugian seperti pencurian informasi.



Gambar 1.2 *New Varian Malware* (*G Data*, 2015)

Sedangkan menurut AV-TEST terdapat 390.000 program berbahaya baru setiap hari dan pada tahun 2016 terdapat rata-rata jumlah sampel *malware* baru setiap hari adalah antara 10.000 –16.000, dari data yang diuraikan terjadi peningkatan jumlah *malware* pada 12 bulan terakhir (av-test.org)



Gambar 1.3 *New sample Malware* (*Av-Test.org*, 2016)

Program berbahaya atau *malware* menjadi sebuah ancaman atau masalah yang sulit bagi para peneliti, tidak ada *platform* komputasi atau lingkungan yang kebal terhadap ancaman tersebut, secara tradisional *malware* dianggap sebagai *virus* atau *worm* yang memiliki fungsi tunggal atau *payload*. Seiring dengan evolusi dan perkembangannya, *malware* dapat

menggabungkan beberapa *vector* untuk melakukan infeksi, contohnya seperti pada *file hashing* yang dimana *file* tersebut dapat diduplikasi sehingga sangat sulit untuk dilakukan analisis, selanjutnya adalah penggunaan teknik anti-forensik yang digunakan untuk menghambat deteksi, menyamarkan kode sehingga kode tersebut tidak dianggap berbahaya oleh perangkat analisis. Kompleksitas yang meningkat membuat para peneliti harus bekerja keras dan membutuhkan waktu untuk memahami cara kerja *malware* tersebut (Valli and Brand 2008)

Penelitian *malware* masih berfokus pada analisis perilaku hal ini dibuktikan dengan seringnya analisis *malware* dilakukan menggunakan teknik *signature based*, teknik ini digunakan untuk melakukan analisis berbasis pada *database* perilaku *malware*, akan tetapi dalam beberapa penelitian seperti yang dilakukan oleh (Chiang 2016) dan (Jasiul, Szpyrka, and Sliwa 2014) yang menjelaskan bahwa tingkat keberhasilan metode yang diterapkan untuk mendeteksi *malware* tergantung pada keadaan model *malware* tersebut. Penggunaan teknik *signature based* sangat tergantung pada perilaku *malware* yang dianalisis, analisis menjadi sulit ketika *malware* yang dianalisis merupakan *malware* baru yang menggunakan teknik kebingungan *(obfuscation)* dan kompresi *(packing).*

Penelitian yang dilakukan oleh (Chiang 2016) dijelaskan bahwa *mobile malware* telah menyebabkan kerusakan dan bocornya privasi pengguna penipisan daya baterai dan megirim pesan multimudia secara otomatis atau pengendalian jarak jauh serta mengunduh program dari internet dan kemudian dibagikan melalui *bluetooth* untuk menyebarkan dari satu perangkat lainnya, dengan cara melakukan proses menggandakan diri melalui *worm* dengan tidak merubah atau merusak *file* yang ada. Dalam penelitiannya yang menjadi fokus pembahasan adalah membangun sebuah ontologi untuk mendeteksi penyebaran *malware* melalui *bluetooth*, pesan multimedia dengan menganalisis perilaku normal dan tidak normal pada sebuah perangkat *mobile*. Metodologi yang digunakan pada penelitian ini mengadopsi metode yang diusulkan oleh (Gruninger and Fox, 1995) yaitu *Toronto Virtual Enterprise*, dan hasil yang didapatkan dari penelitian ini adalah membangun sebuah ontologi dengan mengusulkan metode baru yang dimulai dengan melakukan ekstraksi pada *signature* perilaku yang kemudian dijadikan sebuah konstruksi ontologi untuk mengelolah pengetahuan perilaku *mobile malware* sehingga dapat membantu para pengguna akhir memahami perilaku dari *mobile malware*.

Penggunaan ontologi untuk melakukan analisis *malware* sangat dibutuhkan dikarenakan ontologi merupakan pendekatan yang digunakan untuk melakukan penggalian data. Saat ini ontologi didefenisikan sebagai kerangka representasi pengetahuan atau basis pengetahuan yang memungkinkan eksplorasi pengetahuan secara eksplisit dan ekspresif dengan sangat baik. (Daconta et al., 2003)

Berdasarkan uraian latar belakang diatas, dan dengan fakta yang disampaikan, peneliti menganggap perlu dibangun sebuah ontologi dalam melakukan analisis *malware* yang mencakup cara kerja *malware,* perilaku, serta karakteristik dengan secara detail dan pengklasifikasian jenis *malware* agar memudahkan para peneliti *malware* dalam melakukan panelitinya serta dapat digunakan sebagai pengemabangan, pemetaan pengetahuan dalam mengindetifikasi tren, pola, cara kerja dan karakteristik sehingga dapat dibedakan antara *subclass malware* dengan jelas dan tepat. Pada penelitian ini metode yang diusulkan adalah pengembangan dari metode *Malware Analysis Body of Knowledge*, dimana metode ini bekerja pada domain tertentu untuk memetakan karakteristik dan mengklasifikasi jenis *malware* yang akan dibahas pada penelitian ini.

Metode penelitian ini sudah pernah diusulkan pada penelitian sebelumnya yang dilakukan oleh (Valli and Brand 2008) akan tetapi pada penelitian sebelumnya hanya menyajikan dasar dari domain pengetahuan sebagai lagkah awal untuk melakukan analisis kemungkinan bidang atau bagian apa saja yang bisa terkontaminasi oleh *malware,* sedangkan pada penelitian ini berfokus kepada ontologi sebagai *knowledge base* dan pembahasannya lebih kepada memetakan karakteristik dan pengkalsifikasian jenis *malware*. Penelitian ini hanya sampai pada konsep ontograf, dikarenakan penerapan analisis *malware* ini lebih ditekankan kepada *knowledge base* sebagai pemetaan pengetahuan dan juga sebagai pengklasifikasian jenis dan karakteristik *malware.* Selain itu ontograf juga merupakan pemodelan ontologi untuk menggambarkan konsep dasar dari pengetahuan yang terintegrasi. Dengan ontograf dapat dilihat hubungan *subclass* dan *tree,* mendukung berbagai penurunan (*multiple inheritence*) dan *roo*t pada *class* yang terbentung yaitu *class "thing".* Ontograf dibuat untuk melihat *class* yang dibuat. (Jurcik 2010).

1.2 Rumusan Masalah

Berdasarkan permasalahan yang telah diuraikan pada latar belakang diatas, adapun rumusan masalah dari penelitian ini yaitu:

a. Bagaimanakah penerapan ontologi sebagai *knowledge base* dasar dalam melakukan analisis karakteristik *malware* ?
b. Bagaimanakah penerapan analisis *malware* dengan metode klasifikasi dan analisis karakteristik *malware* dengan menggunakan ontologi ?

1.3 Batasan Masalah

Untuk lebih fokus dan terarahnya penelitian yang dilakukan dan berdasarkan rumusan masalah yang telah diuraikan sebelumnya, maka peneliti memberikan batasan dalam penelitian ini:

a. Pada penelitian ini hanya membahas bagaimana ontologi analisis *malware*.

b. Kategori *malware* yang dibahas pada penelitian ini adalah *trojan horse, virus, exploit, worm* dan *adware*.
c. Analisis yang dilakukan adalah membahas proses analisis ontologi.
d. Analisis yang dilakukan hanya untuk memetakan klasifikasi dan karakteristik jenis *malware*.
e. Rancangan pemodelan hanya sampai pada tahap ontograf.

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian itu yaitu:

a. Membagun sebuah model berbasis ontologi untuk melakukan analisis karakteristik *malware*.
b. Memberikan hasil penelitian dengan penerapan metode klasifikasi dan analisis karakteristik *malware* menggunakan konsep berbasis ontologi

1.5 Manfaat Penelitian

Berdasarkan latar belakang, rumusan masalah, batasan masalah, dan tujuan dari penelitian yang telah disampaikan pada bagian sebelumnya. Adapun manfaat penelitian yang ingin dicapai pada penelitian ini yaitu membangun sebuah ontologi atau kerangka kerja yang dapat digunakan sebagai landasan untuk melakukan penelitian atau analisis *malware*

1.6 Review Penelitian

Untuk menunjang keterkaitan penelitian, berikut akan dijelaskan beberapa pendapat dari penelitian sebelumnya yang dianggap mendukung penelitian ini.

Perkembangan *malware android* dengan teknik pengemasan menjadi isu yang sangat penting dikalangan para peneliti, dengan menggunakan kode enkripsi menjadikan metode analisis terhadap *malware* menjadi sangat sulit. Pendekatan statis dan dinamis analisis yang sering digunakan belum mampu untuk mengatasinya, pendeteksian *malware android* yang efektif adalah dengan cara melakukan pembongkaran kode untuk membuktikan akurasi, sayangnya masalah ini tidak mudah untuk diatasi. Pengemasan *malware android* sering mengadopsi beberapa pertahanan anti analisis yang kompleks.(B et al. 2012). Hal ini diperkuat oleh (Petsas et al. 2014) pendekatan statis dan analisis metode menjadi sangat terbatas ketika analisis yang dilakukan tidak sempurna, hal ini disebebkan oleh *malware* yang dapat memanipulasi kode dan beradaptasi sehingga dapat menghindari deteksi yang dilakukan oleh sistem.

Dalam penelitian yang diusulkan oleh (Dietzel 2014) dijelaskan bahwa sebuah *malware* canggih dapat beradaptasi dengan baik pada lingkungan bahkan dapat menghidari deteksi oleh sistem dengan menggunakan teknik penyamaran perilaku seolah-olah kode sumber yang sedang dianalisis tidak terdapat kode berbahaya.

Penelitian yang dilakukan oleh (Santos 2013) berfokus pada *file manifest* untuk mendeteksi *malware,* penelitian ini berfokus pada analisis aplikasi yang diunduh pada *android market* yang kemudian dilakukan ekstraksi selanjutnya, diklasifikasikan untuk mengetahui cara kerja dari *malware* pada aplikasi tersebut.

Kemampuan untuk menganalisis perangkat lunak berbahaya atau *malware* menjadi disiplin ilmu yang sangat penting dalam dunia forensik digital. Hal ini karena *malware* menjadi sebuah program yang dikelolah oleh pelaku kejahatan untuk mendapatkan keuntungan. Menganalisa dan mendeteksi *malware* mejadi lebih sulit karena membutuhkan keterampilan yang cukup ketika *malware* tersebut dirancang secara khusus. (Valli and Brand 2008)

Peningkatan aplikasi android juga telah memicu peningkatan program berbahaya yang terdapat pada *device* dan mengakibatkan eksploitasi setiap aktifitas yang dilakukan oleh pengguna. Oleh karena itu adanya kebutuhan untuk mempelajari cara kerja serta pendeteksian *mobile malware* untuk memberikan solusi yang efektif. Pada penelitian ini mambahas tentang isu-isu cara kerja *malware* serta mempelajari sistem pedeteksian pada perangkat berbasis android serta mengusulkan ontologi deteksi *malware* serta manfaat dan kendala dari masing-masing sistem deteksi *malware* yang digunakan (Mas'udetal.2014).

Table 1.1 Review Paper Penelitian

Paper	Isu / Masalah	Metode	Hasil
Seyed Hadi Sadjad dkk (2008)	Penelitian ini membahas pengelompokkan *malware* berdasarkan empat atribut yaitu tujuan, status, operasional dan komunikasi yang kemudian menganalisis karakeristik *malware* dalam keamanan jaringan.	Metode pada penelitian ini memanfaatkan logika *fuzzy* untuk menganalisis karakteristik *malware.*	Menghasilkan *framework* dengan menggunakan *fuzzy* dan *semantic web* untuk mendeteksi *malware* pada sistem keamanan jaringan.
Hsein Der Huang dkk (2010)	Masalah yang diangkat pada penelitian ini adalah terdapat lima ancaman yang terjadi pada keamanan jariangan yang dirancang untuk mendapatkan data pengguna atau data pribadi.	Metode Penelitian menggunakan Taiwan *Malware* Analysis Net (TWMAN).	Mengusulkan sebuah sistem cerdas berbasis ontologi untuk melakukan analisis perilaku *malware.*
Ton ton Hsein De Huang dkk (2013)	Isu yang diangkat pada penelitian ini adalah pendekatan analisis *malware* berdasarkan deteksi heuristik dan teknologi tanda tangan yang menjadi sulit dikarenakan akurasi dari pendekatan ini bergantung pada kemampuan untuk mengenali pola dan model *malware* terutama dalam mengindetifikasi keaslian.	Metdoe yang digunakan pada penelitian ini adalah IT2FLS.	Mengusulkan model ontologi untuk menganalisis analisis perilaku dengan memanfaatkan ontologi fuzzy.
Bartosz Jaisul dkk (2014)	Tingkat keberhasilan metode yang diterapkan untuk mendetaksi *malware* masih bergantung pada *code signature,* akan tetapi *code signature* ini lah yang menjadi celah para *hacker* menggunakan bagian dari kode untuk menyisipkan jenis *malware* baru.	Penelitian ini menggunakan model CP- Net dan PRONTO untuk mendeteksi serangan *malware.*	mengusulkan pendekatan ontologi baru untuk analisis kode berbahaya perilaku *malware* berdasarkan model CP-net untuk menginformasikan para pengguna

			keamanan tentang kegiatan yang mencurigakan diamati dalam sistem dimonitor.
Mario Jino dkk (2014)	Deteksi *malware* berbasis perilaku merupakan sebuah tugas yang sulit, karena tergantung pada pemantauan sistem pada sasaran pada saat deteksi, untuk itu perlu pengetahuan yang lebih dalam agar dapat membedakan berbahaya atau tidaknya sebuah program pada saat deteksi dilakukan.	Metode yang digunakan dalam penelitian ini adalah memanfaatkan ontologi sebagai skenario untuk mendeteksi *malware.*	Disajikan ontologi didasarkan pada perilaku *malware* yang mencurigakan diamati selama infeksi *malware* pada sistem korban. Perbedaan antara ontologi yang diusulkan dan yang sudah ada adalah bahwa hal itu tidak terikat kelas *malware* tradisional, tetapi untuk perilaku berbahaya.
Hsiu Sen Chiang dkk (2016)	Mayoritas perangkat lunak untuk mendeteksi *malware* masih bergantung pada *database signature*, jaringan telepon seluler memiliki karakteristik yang sangat berbeda dalam hal kekuatan pemrosesan yang terbatas, kapasitas penyimpanan dan daya baterai. Penelitian ini mengusulkan sebuah analisis perilaku berbasis ontologi untuk *malware mobile,* dan selanjutnya memberikan informasi tentang *malware mobile* bagi pengguna akhir	Metode yang digunakan pada penelitian ini adalah TOVE Enterprise Modeling method.	Mengusulkan metode jenis baru analisis perilaku untuk *malware mobile*. Metode ini dimulai dengan ekstraksi tanda tangan perilaku kunci dari *mobile malware* dengan menerapkan teori ontologi

Abdul Haris Muhammad (2017)	Pada penelitian ini masalah yang di kemukakan adalah analisis *malware* yang dilakukan oleh Hsiu Sen Chiang dkk (2016) masih tergatung pada perilaku *malware* dengan menggunakan *signature based*, akan tetapi teknik tersebut masih tergantung pada model *malware* yang ditemukan, ketika *malware* dengan teknik tidak terdapat pada *database* yang dimiliki maka, akan menjadi sulit untuk melakukan deteksi atau antisipasi. Untuk itu solusi yang ditawarkan adalah membangun sebuah model ontologi karakteristik *malware* sehingga dapat dijadikan sebagai landasan dan pengemabangan, dalam melakukan analisis *malware*	Penelitian ini menggunakan pengembangan metode *Malware Analisis Body Of Knowledge* dengan menjadikan ontologi sebagai basis pengetahuan, dengan memiliki tujuh tahapan yaitu *Ethical / Low*, *Data Collection*, *Methodology Analysis*, *Classification and Analysis Characteristic Malware*, *Ontology*, *Post Assessment Malware* dan *Malware Characteristic Ontology*	Hasil dari penelitian ini adalah sebuah ontologi karakteristik *malware*

1.7 Metode Penelitian

Adapun langkah-langkah yang akan ditempuh selama melakukan penelitian ini yaitu sebagai berikut:

a. Studi Literatur

Penelitan ini dilakukan dengan melakukan studi keputsakaan yaitu dengan mengumpulkan bahan-bahan referensi yang terkait dengan penelitian, baik melalui buku, jurnal, artikel, paper, malakah

b. Analisis

Analisis dilakukan pada proses analisis *malware* sebagai masukan atau input yang kemudian dilakukan analisis terhadap metodologi, klasifikasi deteksi *malware* serta proses hasil atau output berdasarkan pertimbangan perspektif hukum dan etika.

c. Perancangan

Pada tahap ini peneliti memberikan rancangan terkait pengembangan metode dalam membangun sebuah ontologi atau kerangka kerja untuk memetakan pengetahuan dalam melakukan analisis *malware*

d. Implementasi

Tahap implemetasi yang dimaksud adalah mengimplementasi hasil dari proses analisis dan pengembangan metode sehingga menghasilkan sebuah ontologi atau kerangka kerja baru dalam melakukan analisis *malware*

e. Laporan

Tahap laporan adalah tahapan akhir dari pelaksanaan penelitian ini, yaitu penyampaian kesimpulan atas terbentuknya sebuah ontologi analisis *malware* baru yang digunakan dalam melakukan pemetaan pengetahuan yang dibutuhkan dalam melakukan analisi *malware.*

1.8 Sistematika Penulisan

Tahapan ini adalah tahapan yang memberikan gambaran secara umum terkait dengan sistematika penulisan, dengan tujuan memberikan penjelasan secara ringkas terhadap kerangka dalam penulisan.

BAB I: PENDAHULUAN

Tahapan ini adalah tahapan awal yang dilakukan dalam penelitian tahapan ini berisikan penjelasan terkait dengan latar belakang penelitian, penetapan judul, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, serta sistematika penulisan yang dilakukan.

BAB II: LANDASAN TEORI

Pada tahapan ini membahas tentang beberapa teori yang mendukung dalam penelitian yang dilakukan, terkait dengan *malware* dan ontologi.

BAB III: METODOLOGI

Tahapan ini berisikan gambaran secara umum tentang analisa, struktur serta proses perancangan sebuah ontologi dengan menggunakan metodologi

BAB IV: IMPLEMENTASI

Tahapan ini membahas tentang mengimplementasi hasil dari proses analisis dan pengembangan metode sehingga menghasilkan sebuah ontologiatau kerangka kerja baru dalam melakukan analisis *malware.*

BAB V: KESIMPULAN DAN SARAN

Tahapan ini adalah tahapan terakhir yang dilakukuan dalam penelitian ini dan memuat tentang kesimpulan dari keseluruhan uraian dari Bab-bab sebelumnya, serta memberikan saran terkait dengan kekurangan yang diperoleh dalam penelitian untuk pengembangan ilmu pengetahuan