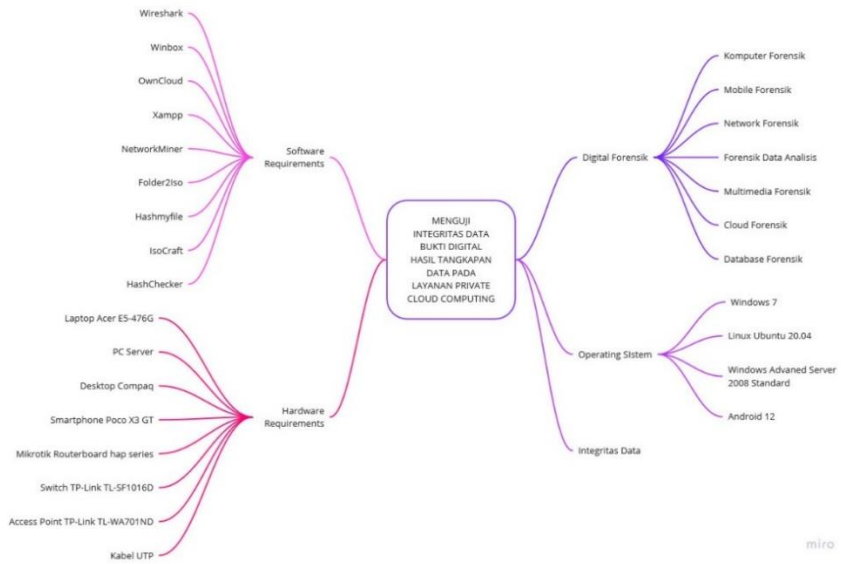
BAB II

LANDASAN TEORI



Gambar 2. 1 Mind Maps

Gambar 2.1 *Mind Map* mengenai teori yang berkaitan dengan penelitian ini. Penelitian ini berlangsung pada *cloud forensics* yang mana merupakan bagian dari digital forensik, menggunakan metode *Digital Forensics Investigation Framework (DFIF)* tahapan pada *framework* yang digunakan meliputi pengumpulan, atau *collection*, pemeriksaan atau *examination*, analisis atau *analysis*, laporan dan dokumentasi atau *reporting and documentation,* objek penelitian dilaksanakan pada *server owncloud* pada system operasi *windows advanced server 2008 standard*, serta beberapa *client* dengan system operasi, *windows 7* yaitu *desktop compaq presario v3500* , *linux ubuntu 20.04* yaitu *laptop acer e5-476g*, serta *android 12* yaitu *poco x3 gt*, dan beberapa perangkat tambahan seperti *mikrotik*, *swith*, *access point* serta kabel *utp* sebagai perangkat yang digunakan untuk menghubungkan jaringan lokal.

2.1 Integritas Data

Integritas data merupakan salah satu aspek keamanan data, bertujuan untuk menjamin keaslian dan keutuhan data, sehingga bisa melindungi perubahan data dari pihak lain yang tidak memiliki wewenang (Andy and Rahardjo, 2016), perubahan tersebut berupa penyisipan, menghapus dan mengganti data yang lain ke dalam data yang asli.

2.2 *Cloud Computing*

National Institute of Standards and Technology (NIST) menerangkan bahwa definisi *cloud computing* merupakan sebuah skema untuk mewujudkan kenyamanan dalam akses jaringan *on-demand* sehingga dapat melakukan konfigurasi secara bersama pada kumpulan berbagai layanan seperti layanan jaringan, apliksi, media penyimpanan, *server* atau pun penyedia layanan (Psannisd kk., 2019), *cloud computing* memiliki lima karakteristik (Febrian et al., 2016), yaitu

1. *On-demand self-service*

   Pengguna *cloud computing* menentukan kinerja dari *cloud computing* sesuai keperluan organisasi seperti *server time*, *network storage* tanpa perlu melakukan interaksi dengan penyedia layanan, sehingga menjadi efektif dan efisien dalam melakukan tugas.

2. *Broad network access*

   Kemampuan layanan terhubung melalui jaringan dan dapat digunakan secara layak melalui berbagai *platform* seperti *handphone*, tablet, laptop maupun tempat kerja.

3. *Resourcer pooling*

   Penyedia layanan *cloud computing* memusatkan berbagai layanan sumber daya dalam satu *data center* terdiri dari berbagai server yang berbeda, serta mekanisme kinerja dilakukan sesuai dengan permintaan konsumen, sumber daya layanan ini meliputi penyimpanan, pemrosesan, *memory*, *bandwith* jaringan serta mesin *virtual*.

4. *Rapid elasticity*

   Penetapan layanan dilakukan secara elastis, dalam beberapa masalah dapat terselesaikan secara otomatis sehingga mempercepat perhitungan keluar masuk sesuai permintaan, atau pengurangan dan pertambahan suatu penyimpanan sehingga dapat dilakukan secara cepat.

5. *Measured service*

   Layanan *cloud computing* secara otomatis bisa mengoptimalkan penggunaan sumber daya, dengan menggunakan sistem pengukuran dapat digunakan sebagai pengawasan berbagai layanan seperti penyimpanan, pemrosesan, *bandwith,* serta *user* aktif, dengan demikian pengawasan tersebut memiliki transparansi bagi penyedia dan konsumen dari layanan yang dipergunakan.

Layanan *cloud computing* terbagi menjadi tiga jenis layanan, yaitu:

1. *Software as a Service (IaaS),* Layanan ini menawarkan *cloud computing* tanpa harus mempersiapkan infrastruktur dari *cloud computing* seperti *server*, jaringan, sistem operasi maupun konfigurasi lainnya, layanan ini dapat digunakan menggunakan berbagai perangkat *client* seperti antarmuka *web browser* maupun aplikasi *android.*

2. *Platform as a Service (PaaS),* Layanan ini menawarkan keleluasaan kepada pengguna yaitu dapat menggunakan aplikasi yang dibuat oleh pengguna itu sendiri sesuai yang dibutuhkan organisasi, menggunakan bahasa pemrograman yang didukung oleh penyedia layanan, sama seperti layanan *Software as a Service (IaaS),* layanan ini tidak dapat melakukan konfigurasi mendasar severti *server*, jaringan, penyimpanan, sistem operasi maupun konfigurasi lainnya.
3. *Infrastructure as a Service (IaaS),* Layanan ini memiliki keleluasaan lebih bagi pengguna karena dapat mengelola komputasi yang penting serta dapat melakukan penyebaran dan menjalankan aplikasi secara bebas, pengguna tidak melakukan konfigurasi mendasar namun memiliki kontrol terhadadap sistem operasi, penyimpanan, aplikasi yang digunakan untuk membuka layanan, serta konfigurasi terbatas seperti *firewall.*

Penyebaran *cloud computing* terdiri dari empat jenis yaitu:

1. *Private cloud.*
2. *Public cloud.*
3. *Community cloud.*
4. *Hybrid cloud*

2.3 *Private Cloud*

Merupakan cabang dari *cloud computing, private cloud* hampir sama dengan *public cloud* memiliki layanan yang dikelola sendiri, dijalankan oleh suatu organisasi itu sendiri, layanan ini dibuat untuk kebutuhan internal organisasi, sehingga pekerjaan lebih efektif serta menghemat pengeluaran (Deepa and Cheelu, 2018).

2.4 Digital Forensik

Digital forensik adalah prosedur yang dilakukan untuk mencari, melakukan analisa pada perangkat digital menggunakan *software* dan *tools* serta melakukan ekstrak dan memelihara bukti digital dengan tujuan mendapatkan bukti dari tindak kejahatan serta menjaga keaslian *file* bukti digital (Putra et al., 2018). Digital forensik memiliki cabang ilmu terdiri dari *computer forensics*, *mobile forensics*, *audio forensics*, video *forensics* serta *image forensics* (Wijanarko and Prakarsa, 2021).

1. *Computer Forensics*, Cabang ilmu ini berhubungan dengan investigasi bukti digital dan elektronik pada komputer atau media penyimpanan digital, dengan cara memeriksa perangkat perangkat komputer, bertuiuan untuk mengumpulkan, memulihkan, melakukan analisa berbagai bentuk bukti yang berhubungan dengan komputer (Moedjahedy, 2016).
2. *Mobile Forensics*, Cabang ilmu digital forensik, suatu teknik yang digunakan untuk mengumpulkan, melakukan analisa serta memulihkan bukti digital yang berhubungan dengan perangkat seluler (Zamroni et al., 2016).
3. *Audio Forensics*, Ilmu cabang digital forensik yaitu teknik menganalisa bukti digital dengan bentuk suara atau rekaman, seperti memecahkan bukti digital rekaman suatu percakapan, tahapan dari *audio forensics* terdiri dari, akuisisi, analisa, evaluasi serta presentasi (Huizen et al., 2016).
4. *Video Forensics*, Ilmu cabang dari digital forensik bertujuan untuk melakukan analisa terhadap bukti digital berbentuk video, seperti melakukan identifikasi keaslian video pembunuhan berencana, sehingga bukti bisa menjelaskan bahwa

video tersebut sesuai dengan kejadian aslinya (Umar et al., 2019).

5. *Image Forensics*, Cabang ilmu ini hampir sama dengan *video forensics*, tetapi analisa dilakukan pada gambar, seperti melakukan identifikasi keaslian suatu gambar pada bukti digital.

2.5 *Cloud Forensics*

Cloud forensics adalah teknik dalam melakukan identifikasi serta analisis tindak kejahatan pada penyimpanan *cloud*, istilah *cloud forensics* pertama dikemukakan oleh (Ruan, K., Carthy, J., Kechadi, T., & Crosbie, 2011) menyebutkan bahwa *cloud forensics* merupakan penerapan dari illmu digital forensik pada lingkungan komputasi awan atau *cloud computing*, secara teknis *cloud forensics* memiliki pendekatan *hybrid* seperti contohnya adalah jaringan, langsung, virtual, secara organisasi. *Cloud* melibatkan beberapa pihak seperti penyedia *cloud*, pengguna *cloud* serta pihak lainnya, tujuan dari investigasi *cloud* forensik ini untuk membantu menelusuri bukti digital yang terjadi pada kasus *cloud computing* sehingga membantu pada persidangan(Hemdan and Manjaiah, 2017).

2.6 *Digital Forensics Investigation Framework (DFIF)*

Penelitian ini menggunakan metode analisa forensik dari *Digital Forensics Investigation Framework (DFIF)*. Penggunaan metode ini sebagai pedoman pada penelitian yang dilakukan sehingga alur penelitian dapat terselesaikan secara sistematis serta dapat membantu menyelesaikan masalah yang ada. Kerangka kerja dari metode *Digital Forensics Investigation Framework (DFIF)* terdari dari empat tahap (Febrian et al., 2016), yaitu:

1. Pengumpulan (*Collection),* yaitu mengumpulkan berbagai data pendukung seperti perangkat yang digunakan oleh pelaku, serta *server* yang nantinya akan dilakukan pemeriksaan terhadap perangkat tersebut untuk mencari bukti digital pada setiap perangkat.
2. Pemeriksaan (*Examination*), yaitu mengumpulkan berbagai bukti digital yang ada pada perangkat pelaku dan *server* untuk medukung proses penyelidikan, seperti lokasi penyimpanan bukti digital, *traffic* jaringan pada *layer* 5 menggunakan *wireshark* serta *network mine*, serta melakukan *cloning* terhadap bukti digital yang didapatkan sehingga meminimalisir perubahan pada bukti digital.
3. Analisis (*Analysis*), memeriksa bukti digital yang didapatkan pada proses pemeriksaan (*Examination)* baik bukti digital asli maupun hasil *cloning*, analisis dilakukan yaitu dengan cara melakukan pengujian nilai *hash* dari setiap file asli, serta pengujian nilai *hash* sesudah akusisi bukti digital, lalu melakukan perbandingan dari proses tersebut.
4. Dokumentasi dan Laporan (*Reporting and Documentation*), yaitu menguraikan serta menjelaskan kesimpulan dari identifikasi yang telah dilakukan, kemudian dimasukan pada laporan teknis.

2.7 *Operating System*

Operating system atau dalam bahasa Indonesia sering disebut sitem operasi adalah perangkat lunak lapisan pertama pada penyimpanan baik pada komputer maupun pada *smartphone,* sistem operasi melakukan kinerja sebagai pengelola semua aktifitas dari perangkat yang berhubungan dengan *hardware* atau perangkat

keras, seperti penjadwalan proses, pengolahan aplikasi, sistem operasi sangat penting bagi suatu perangkat hal ini dikarenakan jika tidak ada sistem operasi makan perangkat komputer atau *smartphone* tidak akan berguna, contoh dari beberapa sistem operasi adalah *Windows Server/7/8/10*, *Linux* yang didalamnya terdapat cabang yaitu sistem Operasi *Android s*erta *MacOS*(Josi, 2019).

2.8 *Packet Analyzer*

Packet Analyzer adalah *tools* yang digunakan untuk analisis *traffic* jaringan internet, perangkat lunak ini mampu mendeteksi berbagai aktivitas pada jaringan seperti memonitoring jaringan, mendeteksi aktivitas serangan sehingga bisa melakukan pencegahan (Hanipah and Dhika, 2020), perangkat lunak ini dapat dipakai dalam berbagai sistem operasi seperti *linux, macOS* ataupun *windows.* Perangkat lunak ini dapat diunduh oleh siapa secara gratis karena aplikasi *freeware*. Beberapa contoh *software packet analyzer* adalah *wireshark* dan *Network Miner.*

2.9 *OwnCloud*

Owncloud merupakan salah satu dari perangkat lunak *cloud computing*, perangkat lunak ini berfungsi sebagai media untuk mengelola maupun menyimpan data berbasis web yang dapat digunakan secara gratis, perangkat lunak ini memiliki keamanan yang baik serta memiliki *interface* yang baik bagi pengguna sehingga mudah digunakan dalam berbagi data dan penyimpanan data (Istanto et al., 2021).

2.10 *XAMPP*

XAMPP kepanjangan dari X (*croos platform),* A (*Apache),* M (*MySQL/MariaDB),* P (*PHP)* serta P (*perl), software* ini merupakan paket dari aplikasi yang ada pada namanya yaitu, *Apache*, *Mysql/MariaDB, PHP* dan *perl*, *XAMPP* sudah satu paket dan sudah terpasang secara otomatis sehingga lebih memudahkan karena tidak perlu melakukan konfigurasi terhadap masing masing perangkat lunak, *XAMPP* berbasis *open source* dan *freeware*.

2.11 *Switch*

Switch merupakan perangkat keras yang ada pada jaringan internet, memiliki fungsi untuk menghubungkan beberapa perangkat komputer agar terhubung dengan jaringan lokal yang dibuat sehingga dapat melakukan pertukaran data antar komputer yang terhubung menggunakan *switch*, pada dasarnya *switch* hamprr sama dengan *hub* yang membedakan adalah kinerja *switch* yaitu mengirim paket langsung ke *ip* tujuan sehingga lebih cepat dan effisien, sementara hub mengirimkan ke semua komputer sehingga kinerjanya lebih lambat.

2.12 *Access Point*

Accees point adalah perangkat keras yang digunakan pada jaringan lokal untuk mengirim dan menrima data, perangkat ini merupakan penghubung antara pengguna dalam jaringan dan berfungsi sebagai titik konektifitas data baik *wireless* maupun menggunakan kabel utp. *Access point* terdapat antenna *transceiver* berfungsi untuk menyebarkan koneksi dari *client server* maupun menuju *client server* sehingga dapat menyebarkan konektivitas *wifi*.

2.13 *Imaging tools*

Kebihan menggunakan *tools imaging* adalah proses penyalinan sama persis seperti aslinya sehingga file yang disalin tidak terdapat perubahan, hasil dari penyalinan tersebut berformat *.iso, .daa, .img, .bin,* serta format yang lainnya, penelitian menggunakan beberapa *tools* untuk melakukan imaging yaitu pada sistem operasi *windows* dan *linux* menggunakan *folder2iso* sementara pada sistem operasi *android* menggunakan aplikasi *IsoCraft* dalam akusisi bukti digital pada setiap perangkat.

2.14 *Hash Checker*

Kalkulator *hash* adalah program yang berfungsi untuk menampilkan *hash* pada sebuah data, *hash* merupakan nilai yang berupa apa saja mulai dari angka maupun *string* dari ratusan karakter alfanumerik, bergantung algoritma mana yang digunakan, pada kalkulator setiap menampilkan nilai *hash* suatu *file* beberapa kali, nilai *hash* akan bernilai sama hal ini dikarenakan fungsi *hash* harus stabil. Penelitian ini menggunakan beberapa aplikasi untuk menguji nilai *hash* dari suatu *file, tools* yang digunakan pada *windows* yaitu *freeware HashMyFile* sementara pada *android* menggunakan *HashChecker*.

2.15 *State of Art* Penelitian Investigasi serta menguji integritas data

Tabel 2.1 menunjukan perbandingan penelitian sebelumnya yang berhubungan dengan penelitian pengujian integritas pada *cloud forensik* pada tangkapan data pada *private cloud*. Terdapat beberapa kesamaan serta perbedaan dari penelitian. Hal ini dapat dilihat dari penggunaan metode serta algoritmanya.

Tabel 2. 1 *State of Art* Penelitian terkait

No	Peniliti	Judul	Metode	*Tools*	Hasil
1	Irfan Febrian Editia Kurdiat, Nur Widiyasono & Husni Mubarok (2016)	Analisi Proses Investigasi *Dekstop PC* yang Terhubung Layanan *Private Cloud.*	*End to End Digital Investigation (EEDI)*	*Belkasoft Evidence Center* *DumpIt* *Folder2Iso* *Passwordfox* *MD5 & SHA-1 Checksum Utility* *OwnCloud* *mIRC*	• Penelitian dilakukan pada *Desktop PC* yang terhubung layanan *Private Cloud* • Sekenario pelaku dilakukan pada *browser, owncloud,* aplikasi *chatting mIRC* serta *virtual memory* • Penelitian menggunakan *tools Belkasoft Evidence Center, DumpIt, Folder2Iso, Passwordfox, MD5 & SHA-1 Checksum Utility* • Bukti digital menemukan aktivitas pada *cache browser, username password, logs chatting mIRC, email, file* dalam MS Word • Penelitian menggunakan metode *End to End Digital Investigation* (EEDI) pada kasus nyata memiliki kelemahan waktu jika terdapat bukti yang banyak.
2	Nur Hayati, Mohammad Ari Budiman dan Amer Sharif (2017	Implementasi *Algoritma RC4A* dan *MD5* untuk Menjamin *Confidentiality* dan *Integrity* pada *File* Teks	*RC4A* dan *MD5*	Bahasa Pemrograman C# *SharpDevelop versi 4.3*	• Perancangan aplikasi pengaman file *text* dengan menggunakan *algoritma RC4A* • *Algortima MD5* mampu memeriksa keutuhan file *text* dengan cara menghitung nilai *hash* dengan membandingkan dari pengirim

Lanjutan tabel 2.1 *State of Art* Penelitian terkait

No	Peniliti	Judul	Metode	*Tools*	Hasil
3	Nur Widiyasono, Imam Riadi & Ahmad Luthfi (2016)	Penerapan Metode *ADAM* Pada Proses Investigasi Layanan *Private Cloud Computing.*	*The Advance Data Acquisition Model (ADAM)*	*Network Minner* *Wireshark* *WinIso* *Microsoft Windows 2008 Advances Server* *VirtualMachine (Vmware)* *OwnCloud-5.0.5*	• Penelitian dilakukan pada sisi *client* yaitu *smartphone, laptop, desktop pc,* melalui *interntet* ataupun *Local Area Network (LAN)* yang terhubung pada *Private Cloud* • Bukti digital yang ditemukan seperti jenis *file, mac address, username, password, log* dan *timestamp* • Identivikasi bukti digital pada metode *ADAM* dapat dilakukan secara *live* ataupun *write-block* sehingga *realibitas* data dapat dipertanggung jawabkan pada persidangan. • Penyalahgunaan tersebarnya informasi rahasia dikarenakan kelemahan system yang digunakan atau kesalahan konfigurasi dan tidak menggunakan *access policy* pada *private cloud*
4	Didik Sudyana, Nora Lizartia & Erlina (2019)	*Forensic Investigation Framework on Server Side of Private Cloud Computing*	*SNI 27037:2014*	*AccessData FTK Imager* *Apache Log Viewers*	• Penelitian dilakukan pada *owncloud server side* yang terhubung dengan *private cloud.* • Teknik yang digunakan dalam penelitian adalah *Static Forensic* karena investigasi fokus pada data *non-volatile.* • Penelitian berfokus mencari bukti digital perusahaan dan mencari *log server owncloud.*
5	Budi K. Hutasuhut, Syahril Efendi dan Zakarias Situmorang (2019)	*Digital Signature* untuk Menjaga Keaslian Data dengan *Algoritma MD5* dan *Algoritma RSA*	*Algoritma MD5* dan *Algoritma RSA*	*Php* *Google chrome* *Xampp 1.7.3*	• Sekenario dilakukan dengan beberapa percobaan, dan pada tiap percobaan memiliki hasil yang baik pada pengujian integritas • Kombinasi *Algoritma MD5* dan *RSA* sangat baik karena perubahan sedikit saja pada gambar maka *MD5* akan berubah, serta penggunaan algoritma *RSA* mencegah orang untuk dapat menggunakan *digital signature* karena yang bisa hanya yang memiliki *private key*

Lanjutan tabel 2.1 *State of Art* Penelitian terkait

No	Peniliti	Judul	Metode	*Tools*	Hasil
6	Tri Rochmadi (2019)	Deteksi Bukti Digital Pada *Adrive Cloud Storage* Menggunakan *Live* Forensik	*National Institute of Standard and Technology (NIST)*	*FTK Imager* *Autopsy*	• Penelitian dilakukan pada *Cloud Adrive* menggunakan *tools FTK Imager* dan *Autospy* • Metode yang digunakan adalah *National Institute of Standard and Technology (NIST)* dengan teknik *live forensic* investigasi dilakukan saat perangkat yang digunakan pelaku dalam keadaan hidup • Investigasi dilakukan pada *RAM* perangkat dan mendapatkan bukti berupa lokasi instalasi serta *file* bukti digital.
7	Didik Sudyana dan Nora Lizarti (2019)	*Digital Evidence Acquisition System on IAAS Cloud Computing Model using Live Forensic Method*	SNI 27037:2014	*AutoSpy* *Virutal server proxmox* *Mesin virtual windows* *Mesin virtual ubuntu* *Tools* akuisisi bukti digital yaitu rancangan menggunakan Bahasa *bash shell*	• Penelitian dilakukan dengan teknik *Live Forensic* karena akusisi dilakukan pada system yang masih berjalan • *Tools* yang digunakan untuk akuisisi bukti digital menggunakan aplikasi yang dirancang menggunakan Bahasa pemrograman *Bash Shell*, hal ini dikarenakan akuisisi akan dilakukan pada sistem operasi teks berbasis *Linux*. • Simulasi dilakukan dengan menghapus 4 *file* dari *server proxmox*, kemudian akan dianalisa bukti digital menggunakan *tools* rancangan yang dibuat, setelah didapat ekstraksi dianalisa mengguanakan *autopsy*. • Hasil penelitian yaitu pemuliahan data dilakukan menggunakan *Autospy* dan data berhasil dipulihkan serta nial *hash* tetap sama, serta dapat mendeteksi lokasi *partisi* yang digunakan tindak kejahatan.

Lanjutan tabel 2.1 *State of Art* Penelitian terkait

No	Peniliti	Judul	Metode	*Tools*	Hasil
8	Irfan Helmi, Nur Widiyasono & Rohmat Gunawan (2019)	Simulasi Analisis Bukti Digital Pada Layanan *Cloud Computing* Menggunakan Metode *NIST 800-86*	*National Institute of Standard and Technology (NIST)*	*OwnCloud* *Apache Server* *MySQL* *WireShark* *Network Minner* *Magic ISO Maker* *HashCalc* *Chrome Browser*	• Penelitian dilakukan dengan teknik *Live Acquistion* menggunakan *tools wireshark* setelah bukti digital didapatkan dilakukan *physical imaging* menggunakan *magic iso maker* • Sekenario penelitian dilakukan dengan beberapa tahap yaitu *client* mengunduh *file* dari *server*, membuat *file* baru, mengunggah *file*, membagikan *file* ke sesame pengguna *cloud*, menghapus *file*, • Hasil penelitian menggunakan *network minner* berhasil didapatkan jejak dari sekenario tersebut yaitu nama *file* dan *direktori* serta jejak perangkat pelaku seperti *ip address, username dan password, timestamp* serta data lainnya
9	Arif Maulana Komarudin (2022)	Menguji Integritas Data Bukti Digital Hasil Tangkapan Data Pada Layanan *Private Cloud Computing*	*Digital Forensic Investigation Framework (DFIF)*	*OwnCloud* *XAMPP* *Mozila Thunderbird* *Folder2Iso* *HashMyFile* *IsoCraft* *HashChecker* *Hmail server* *Wireshark* *Network Miner*	• Penelitian dilakukan secara *live acquisition* pada saat *server* sedang berjalan dan dilakukan *capture traffic* jaringan menggunakan *wireshark.* • studi kasus adalah simulasi yang dilakukan pada sebuah laboratorium • hasil pengujian nilai *hash* sebelum dilakukan akuisisi dan sesudah akuisisi menunjukan bahwa nilai *hash* tetap sama dan tidak ada perubahan.

Lanjutan tabel 2.1 *State of Art* Penelitian terkait

No	Peniliti	Judul	Metode	*Tools*	Hasil
10	Manuel Luis Belo, Derwin R. Sina dan Yelly Y. Nabuasa (2020)	*Algoritma Md5* Dan *Rc5* Untuk Pengamanan *File Pdf*	*RC5* dan *MD5*	*Nitro Pro*	• Pada pengujian aplikasi pada korelasi koefiensi kunci sama pada pdf berbeda, kunci yang sama tidak berpengaruh karena berbeda tiap struktur binary, korelasi yang dihasilkan nilai rendah 0,205795252 • Perbandingan kolerasi koefisiensi panjang kunci 1-8 karakter tidak berpengaruh terhadap pdf berbeda, menghasilkan nilai rendah 0,24692765 • Sensitivitas kunci dengan merubah 1 karakter kunci mendapatkan bahwa sensitif terhadap perubahan, nilai rendah 0,22421886
11	Farid Daryabar, Ali Dehghantanha & Kim-Kwang Raymond Choo (2016)	*Cloud storage forensics: MEGA as a case study*	*McKemmish and National Institute of Standard and Technology (NIST)*	*TCPDump version 4.5.1* *Wireshark* *0xED for Mac 1.1.3* *Hex Workshop 6.7*	• Hasil penelitian menemukan bahwa pengunduhan dan pengunggahan bukti digital nilai *hash* akan tetap sama, namun terdapat perubahan pada *timestamp.* • Hasil dari analisa lalu lintas jaringan menemukan *url* dan *IP Address* yang digunakan aplikasi, *timestamp*, nama server serta sertifikat penyedia komputasi awan. • Penelitian dilakukan terhadap *Android* dan *iOS*
12	Ermi Suryani Nasution (2019)	Mendeteksi Orisinalitas *File Video* Menerapkan Metode *Md5*	*MD5*	*HexWorkShop* *Hasher Pro*	• Pengambilan data dari video hanya *17 byte* karena jika diambil semua video akan mengalami *error* • *Algoritma MD5* berhasil mendeteksi keaslian dari *video* dengan cara membandingkan nilai *hash* dengan *video* asli, karena tiap ada perubahan maka nilai *hash* akan berubah.

2.16 *Matrik* Penelitian

Tabel 2.2 merupakann ruang lingkup dari penelitian sebelumnya sehingga terlihat lebih jelas metode yang digunakan, perangkat pada penelitian, *tools* serta cakupan dari penelitian terkait.

Tabel 2. 2 *Matrik* Penelitian

No	Peneliti	Judul	Ruang Lingkup																									
			Metode Integritas		Metode Investigasi						*Devices*				*Tools*												Cakupan		
			MD5	*RC4*	*End to End Digital Investigation (EEDI)*	*The Advance Data Acquisition Model (ADAM)*	*SNI 27037:2014*	*National Institute of Standard and Technology (NIST)*	*National Institute of Justice (NIJ)*	*DFIF*	*Server*	*Laptop*	*Desktop*	*Smartphone*	*Hashmyfile*	*HexWorkShop*	*Belkasoft Evidence Center*	*Network Miner*	*AccessData FTK Imager*	*Autospy*	*Oxygen Forensics*	*Mobile edit forensic*	*Folder2iso*	*Tools rancangan*	*IsoCraft*	*HashChecker*	*Wireshark*	*Cloud Forensik*	*Mobile Forensik*	*Komputer Forensik*
1	Irfan Febrian Editia Kurdiat, Nur Widiyasono & Husni Mubarok (2016)	Analisi Proses Investigasi *Dekstop PC* yang Terhubung Layanan *Private Cloud.*			√								√				√										√		

Lanjutan tabel 2.2 Matrik Penelitian

2	Nur Hayati, Mohammad Ari Budiman dan Amer Sharif (2017	Implementasi Algoritma RC4A dan MD5 untuk Menjamin Confidentiality dan Integrity pada File Teks	√	√									√																
3	Nur Widiyasono, Imam Riadi & Ahmad Luthfi (2016)	Penerapan Metode *ADAM* Pada Proses Investigasi Layanan *Private Cloud Computing.*				√						√	√	√		√					√							√		
4	Didik Sudyana, Nora Lizartia & Erlina (2019)	*Forensic Investigation Framework on Server Side of Private Cloud Computing*					√				√								√									√		

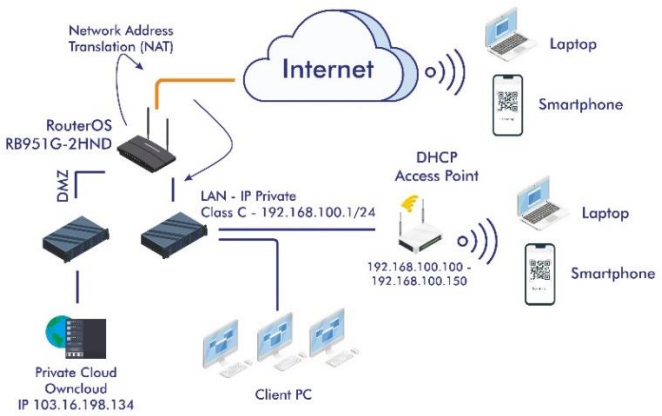
Lanjutan tabel 2.2 Matrik Penelitian

5	Budi K. Hutasuhut, Syahril Efendi dan Zakarias Situmorang (2019)	Digital Signature untuk Menjaga Keaslian Data dengan Algoritma MD5 dan Algoritma RSA	√	√								√	√																	
6	Tri Rochmadi (2019)	Deteksi Bukti Digital Pada *Adrive Cloud Storage* Menggunakan *Live* Forensik						√					√						√	√								√		
7	Didik Sudyana dan Nora Lizarti (2019)	*Digital Evidence Acquisition System on IAAS Cloud Computing Model using Live Forensic Method*					√				√							√		√				√				√		

Lanjutan tabel 2.2 Matrik Penelitian

8	Irfan Helmi, Nur Widiyasono & Rohmat Gunawan (2019)	Simulasi Analisis Bukti Digital Pada Layanan *Cloud Computing* Menggunakan Metode NIST 800-86						√			√																√	√		
9	Arif Maulana Komarudin (2022)	Menguji Integritas Data Bukti Digital Hasil Tangkapan Data Pada Layanan Private Cloud Computing	√	√						√	√	√	√		√			√					√		√	√	√	√		
10	Manuel Luis Belo, Derwin R. Sina dan Yelly Y. Nabuasa (2020)	Algoritma Md5 Dan Rc5 Untuk Pengamanan File Pdf	√	√								√	√																	
11	Farid Daryabar, Ali Dehghantanha & Kim-Kwang Raymond Choo (2016)	*Cloud storage forensics: MEGA as a case study*						√			√								√	√								√		
12	Ermi Suryani Nasution (2019)	Mendeteksi Orisinalitas File Video Menerapkan Metode Md5	√	√								√	√																	

Berdasarkan Tabel 2.1 di atas terdapat beberapa penelitian terdekat yang terkait dengan penelitian sekarang, diantaranya penelitian terdekat pertama berjudul Analisis Proses Investigasi Dekstop PC yang Terhubung Layanan *Private Cloud*, menggunakan metode *End to End Digital Investigation* (EEDI). Penelitian menjelaskan mengenai investigasi pada *desktop* dengan sekenario kasus penyalahgunaan *private cloud* oleh karyawan serta menelusuri jejak kejahatan yang lainnya, tahapan investigasi dengan metode *End to End Digital Investigation* (EEDI) yaitu *Collecting evidence*, *Analysis of individual events, preliminary correlation*, *Event normalizing*, *Event Deconfliction, Second level Correlation, Timeline Analysis, Chain of evidence construction, Corroboration*. Simpulan dari penelitian ini bukti digital dapat dikumpulan dari melakukan analisa aplikasi yang digunakan pelaku, serta *virtual memory*, bukti yang berhasil ditemukan antara lain aktivitas pada *cache browser, username, password, logs chatting mIRC, e-mail* serta *file ms word* (Febrian et al., 2016), berikut skema jaringan yang digunakan pada penelitian (Febrian et al., 2016) pada gambar dibawah.



Gambar 2. 2 Topologi Penelitian Terdekat(Febrian et al., 2016)

Penelitian terdekat yang kedua berjudul Penerapan Metode ADAM Pada Proses Investigasi Layanan *Private Cloud Computing*, penelitian tersebut

menggunakan metode *The Advance Data Acquisition Model (ADAM).* Penelitian ini hampir sama dengan penelitian pertama yaitu penyalahgunaan *private cloud* oleh karyawan, membocorkan data rahasia ke *competitor*, investigasi dilakukan pada *private cloud, network, laptop* serta *smartphone.* Metode *The Advance Data Acquisition Model (ADAM)* pada penelitian tersebut memiliki tiga tahap yaitu Perencanaan Awal (*initial Planning),* Perencanaan di Lokasi (*The On Site Planning)* serta Akuisisi Data Digital (*Acquisition Digital Data*). Simpulan penggunaan metode *ADAM (The Advance Data Acquisition Model)* berhasil dilakukan baik secara *live* atau *write-block acquistion* pada tiap perangkat dan dapat dipertanggungjwabkan pada persidangan (Widiyasono et al., 2016).

Penelitian terdekat selanjutnya berjudul *Forensic Investigation Framework on Server Side of Private Cloud Computing* menggunakan metode *SNI 27037:2014*, sekenario kasus pun sama dengan kedua penelitian terdekat sebelumnya, metode *SNI 27037:2014* memiliki empat tahapan utama yaitu *identification, collection, acquistion* serta *preservation of digital evidance* (Sudyana et al., 2019)

Berdasarkan uraian penelitian terdekat, terdapat persamaan antara penelitian sebelumnya dengan penelitian yang sedang dilakukan, yaitu dilakukan pada *private cloud,* adapun keterbaruan dari penelitian yaitu memiliki perbedaan metode penelitian menggunakan metode *Digital Forensics Investigation Framework (DFIF)* serta dilakukan pengujian terhadap integritas data bukti digital yang ditemukan, penelitian ini bertujuan untuk melakukan pengujian integritas dari *digital evidance* dari tangkapan data pada *private cloud*