

**INVESTIGASI FORENSIK CLOUD IAAS STUDI KASUS  
INFECTED GOOGLE CLOUD VM MENGGUNAKAN METODE  
NATIONALINSTITUTE OF STANDARDSAND TECHNOLOGY  
(NIST)**

**SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Teknik Komputer



disusun oleh

**RAMDANI ILHAM PRATAMA**

**18.83.0273**

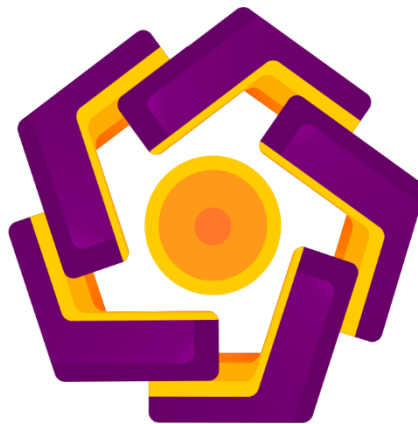
Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2023**

**INVESTIGASI FORENSIK CLOUD IAAS STUDI KASUS  
INFECTED GOOGLE CLOUD VM MENGGUNAKAN METODE  
NATIONALINSTITUTE OF STANDARDSAND TECHNOLOGY  
(NIST)**

**SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Teknik Komputer



disusun oleh

**RAMDANI ILHAM PRATAMA**

**18.83.0273**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2023**

**HALAMAN PERSETUJUAN**

**SKRIPSI**

**INVESTIGASI FORENSIK CLOUD IAAS STUDI KASUS  
INFECTED GOOGLE CLOUD VM MENGGUNAKAN METODE  
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY  
(NIST)**

yang disusun dan diajukan oleh

**Ramdani Ilham Pratama**

**18.83.0273**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 15 Agustus 2023

**Dosen Pembimbing,**



**Banu Santoso, S.T., M.Eng.**

**NIK. 190302327**

HALAMAN PENGESAHAN

SKRIPSI

INVESTIGASI FORENSIK CLOUD IAAS STUDI KASUS  
INFECTED GOOGLE CLOUD VM MENGGUNAKAN METODE  
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY  
(NIST)

yang disusun dan diajukan oleh

**Ramdani Ilham Pratama**

**18.83.0273**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 15 Agustus 2023

Susunan Dewan Penguji

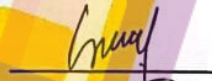
Nama Penguji

**Alva Hendi Muhammad, S.T., M.Eng., Dr.**  
NIK. 190302493

**Senie Destya, M.Kom.**  
NIK. 190302312

**Banu Santoso, S.T., M.Eng.**  
NIK. 190302327

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 15 Agustus 2023

DEKAN FAKULTAS ILMU KOMPUTER



**Hanif Al Fatta, S.Kom., M.Kom.**  
NIK. 190302096

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ramdani Ilham Pratama  
NIM : 18.83.0273

Menyatakan bahwa Skripsi dengan judul berikut:

**Investigasi Forensik Cloud IaaS Studi Kasus Infected Google Cloud VM Menggunakan Metode NIST**

Dosen Pembimbing : Banu Santoso, S.T., M.Eng.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 15 Agustus 2023

Yang Menyatakan,



Ramdani Ilham Pratama

## HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT atas limpahan rahmat dan hidayah serta karunia-Nya sehingga skripsi ini selesai dengan sebaik-baiknya. Skripsi ini saya persembahkan untuk :

1. Ibu dan Bapak saya, Ibu Renti Marini Dan Bapak Eko Erianto yang selalu mendoa'kan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak Banu Santoso, S.T., M.Eng selaku dosen pembimbing yang telah membantu dalam penyusunan skripsi ini.
3. Kepada sahabat dan teman-teman yang ada disaat suka maupun duka selama masa perkuliahan saya.

## KATA PENGANTAR

Puji dan syukur dipanjatkan kehadirat Tuhan Yang Maha Esa atas karunia yang telah dianugerahkan kepada penulis, sehingga penulis dapat menyelesaikan skripsi yang berjudul “Investigasi Forensik Cloud IaaS Studi Kasus Infected Google Cloud Vm Menggunakan Metode NIST”. Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, skripsi ini tidak mungkin dapat terselesaikan. Oleh karena itu, penulis menyampaikan terima kasih kepada :

4. Allah SWT karena atas karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan semoga dapat memberikan manfaat di kemudian hari.
5. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
6. Bapak Dony Ariyus, M. Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
7. Bapak Banu Santoso, S.T., M.Eng selaku Dosen Pembimbing yang telah bersedia memberikan pengarahan dan bimbingan dalam penyusunan Skripsi ini.
8. Segenap Dosen, Staff, dan Karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis di bangku kuliah dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.
9. Orang tua, saudara-saudara beserta keluarga yang selalu mendoakan dan memberikan dukungan penuh kepada penulis.

10. Serta kepada semua pihak yang telah membantu dalam penyusunan Skripsi ini yang tidak dapat penulis sebutkan satu per satu.

Penulis berharap semoga skripsi ini dapat bermanfaat bagi semua pihak yang terkait dalam penulisan ini. Dalam penulisan skripsi ini penulis menyadari masih banyak kekurangan karena terbatasnya pengetahuan dan pengalaman penulis. Karena itu, dengan lapang hati penulis mengharapkan kritik dan saran yang membangun guna menyempurnakan skripsi ini.

Yogyakarta, 15 Agustus 2023

Ramdani Ilham Pratama





## DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	iv
KATA PENGANTAR.....	vi
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
DAFTAR LAMBANG DAN SINGKATAN.....	xiv
DAFTAR ISTILAH.....	xv
INTISARI.....	xvi
ABSTRACT.....	xvii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	4
1.6 Sistematika Penulisan.....	5
BAB II LANDASAN TEORI.....	6
2.1 Tinjauan Pustaka.....	6
2.2 Digital Forensic.....	10
2.3 <i>Standard Operating Procedure (SOP)</i> .....	11
2.4 Bukti Digital.....	11
2.5 Indicators of Compromise (IOC).....	11
2.6 <i>Network Forensic</i> .....	11
2.7 <i>Live Forensic</i> .....	12
2.8 <i>Disk Forensic</i> .....	12
2.9 Layanan Google Cloud.....	13
2.9.1 VPC Flow Logs.....	13

2.9.2	Virtual Hard Disk (VHD).....	13
2.10	NIST <i>Framework</i> .....	14
2.10.1	<i>Collection / Acquisition</i> .....	14
2.10.2	<i>Examination</i> .....	15
2.10.3	<i>Analysis</i> .....	15
2.10.4	Reporting.....	16
2.11	Web Path Brute force.....	16
2.12	Port Scanning.....	17
2.13	SSH Brute force.....	17
<b>BAB III METODE PENELITIAN</b> .....		18
3.1	Alur Penelitian.....	19
3.2	Skenario kasus Serangan.....	20
3.3	Identifikasi Kebutuhan Layanan Google Cloud.....	21
3.3.1	Kebutuhan <i>Service Cloud</i> .....	21
3.3.2	Kebutuhan Perangkat Lunak.....	23
3.4	Alur Investigasi dan Metode Analisis.....	23
<b>BAB IV PEMBAHASAN</b> .....		25
4.1	Persiapan.....	25
4.1.1	Persiapan Lingkungan <i>Cloud</i> .....	25
4.1.1.1	Pembuatan VM Instances.....	26
4.1.1.2	Persiapan Virtual Machine Target.....	27
4.1.1.3	Konfigurasi VM Investigator.....	28
4.1.2	Implementasi Serangan.....	29
4.1.2.1	Information Gathering.....	29
4.1.2.2	Exploitation (Exploit Webmin).....	31
4.1.2.3	Post Exploitation.....	32
4.1.3	Isolasi Jaringan.....	34
4.2	Akuisisi Data (Collection).....	35

4.2.1 Akuisisi Data Traffic Network.....	35
4.2.2 Akuisisi Disk Instance .....	37
4.2.3 Akuisisi Memori RAM .....	42
4.3 Eksaminasi.....	43
4.3.1 Eksaminasi <i>Flow Logs</i> .....	44
4.3.2 Eksaminasi <i>Snapshot Disk Volume</i> .....	45
4.3.2.1 Mount Snapshot Disk.....	46
4.3.2.2 Pembuatan Filesystem Timeline .....	46
4.3.3 Eksaminasi Memori Image.....	47
4.3.3.1 Pembuatan Volatility Profile.....	47
4.4 Analisis Bukti Digital .....	48
4.4.1 Analisis <i>Flow Logs</i> dan Memahami Pola <i>Traffic</i> .....	48
4.4.1.1 Analisis Data Packet Transferred.....	49
4.4.1.2 Analisis Data Traffic pada Port/Protokol.....	49
4.4.1.3 Analisis Data Traffic dari Masing Masing Source IP .....	50
4.4.2 Analisis Snapshot Disk.....	52
4.4.2.1 Analisis Timeline File System .....	53
4.4.2.2 Analisis Log Files .....	54
4.4.3 Analisis Memori Image.....	57
4.5 Laporan Akhir Investigasi (Reporting).....	59
BAB V PENUTUP .....	62
5.1 Kesimpulan .....	62
5.2 Saran .....	62
REFERENSI .....	64

## DAFTAR TABEL

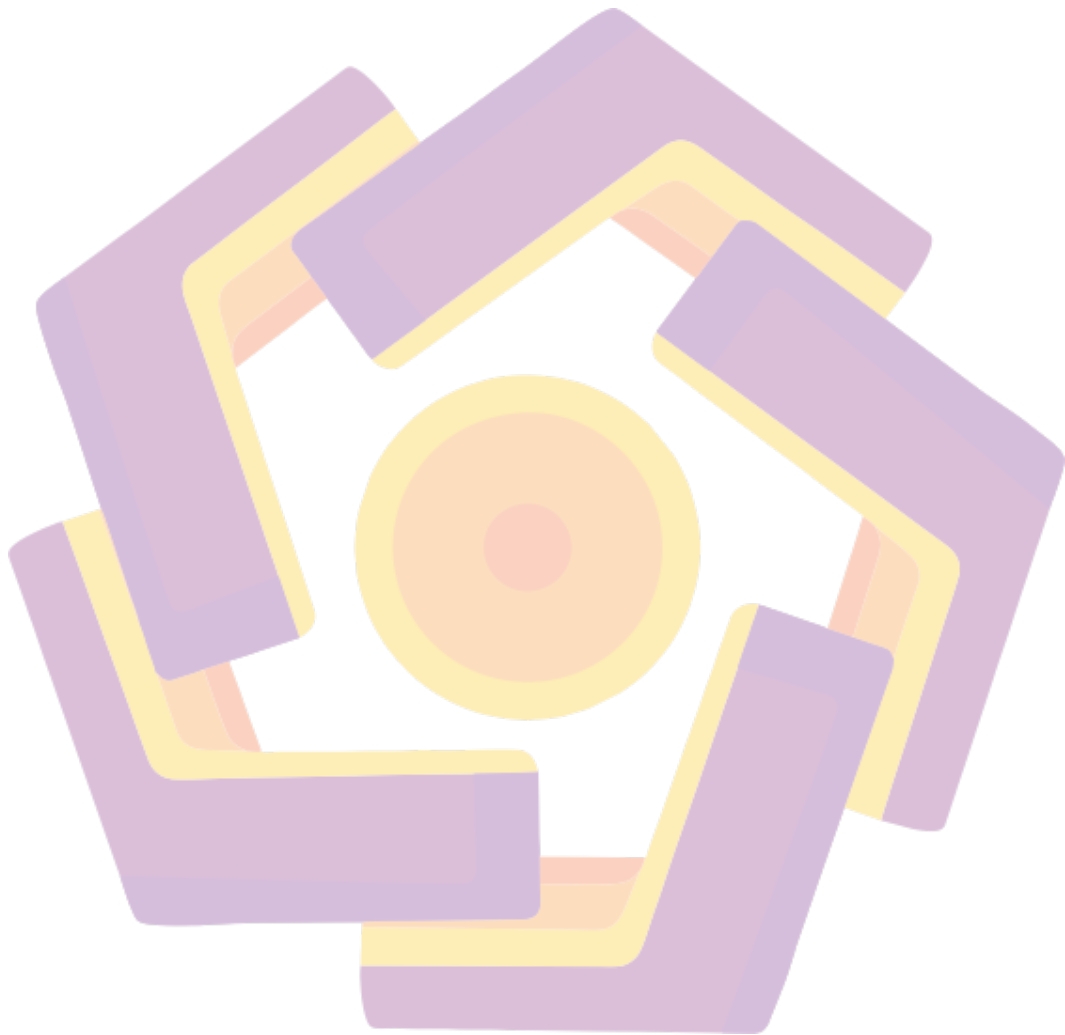
Tabel 2.1 Penelitian Terdahu	6
Tabel 3.1 Perbedaan Perolehan data On-Premise dengan Google Cloud based	16
Tabel 3.2 Dua Tahap Skenario Serangan	17
Tabel 3.3 Spesifikasi VM	18
Tabel 3.4 Kebutuhan Tool Investigasi	19
Tabel 4.1 Informasi Jaringan VM Instance	23
Tabel 4.2 Implementasi Information Gathering dan Exploitation	26
Tabel 4.3 Implementasi Post Exploitation	28
Tabel 4.4 Indikasi Kecurigaan IP Address Threat Actor	44
Tabel 4.5 Indikasi Waktu Serangan Awal Terjadi	44
Tabel 4.6 Temuan Aktivitas Menarik Pada Filesystem Timeline	47
Tabel 4.7 Laporan Akhir Analisis Indikasi Serangan Tahap Awal	50
Tabel 4.8 Laporan Akhir Analisis Indikasi Serangan Tahap Post Exploitation	51



## DAFTAR GAMBAR

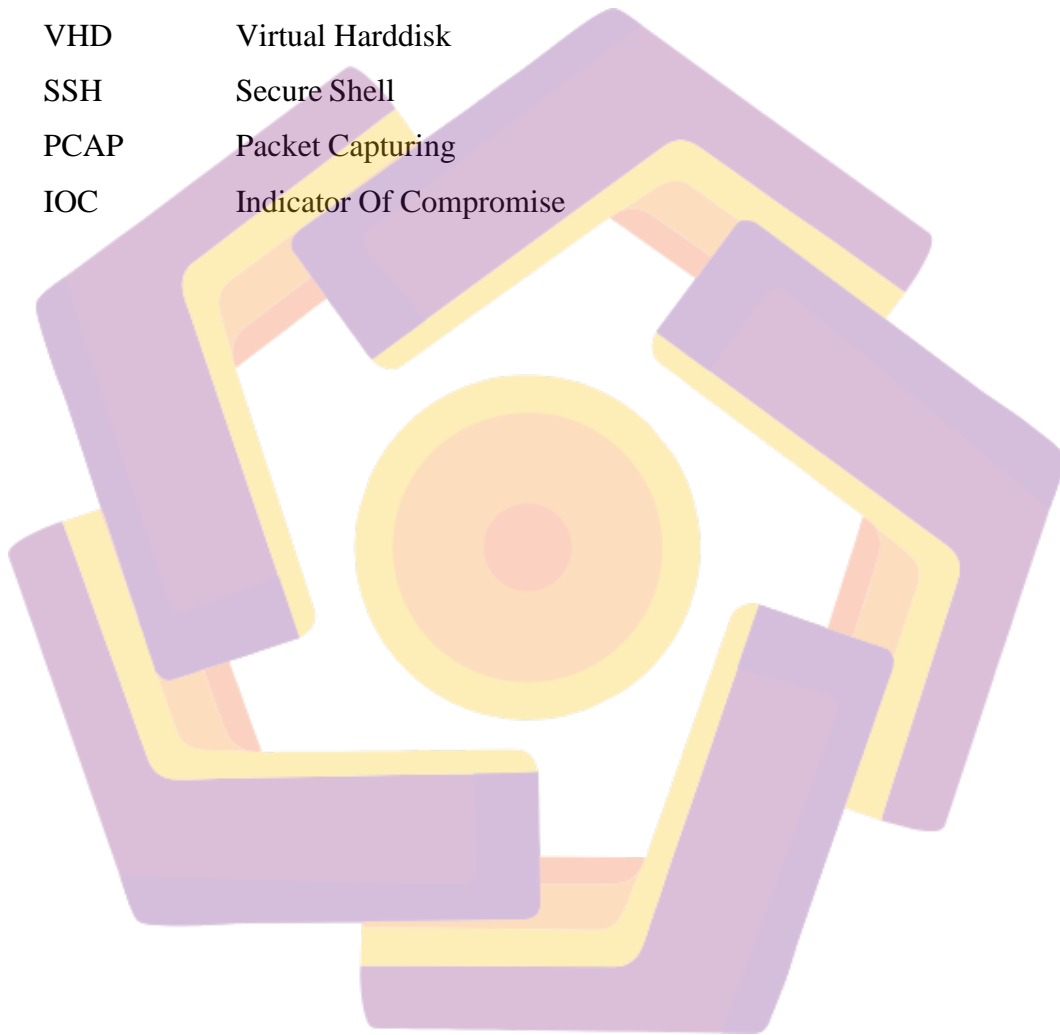
Gambar 1.1 Public Cloud Market Share	2
Gambar 1.2 Data Survey metode penyerangan siber	2
Gambar 3.1 Model Layanan Pada Platform Cloud	17
Gambar 3.2 Alur Penelitian	21
Gambar 3.2 Alur Investigasi Forensik	21
Gambar 4.1 Skenario Penelitian	22
Gambar 4.2 Pembuatan 2 VM Instance	23
Gambar 4.3 Vulnerability Web App	24
Gambar 4.5 Tool dd pada VM Investigator	25
Gambar 4.6 Port Scanning Menggunakan NMAP	26
Gambar 4.7 Skenario Serangan SSH Bruteforce	27
Gambar 4.8 Skenario Serangan Bruteforce Menggunakan ffuz	27
Gambar 4.9 Eksploitasi Webmin	28
Gambar 4.10 Enumerasi Sistem Target	29
Gambar 4.11 Pemasangan Backdoor Pada VM Target	29
Gambar 4.12 Menjaga Akses Dengan Membuat User Baru	30
Gambar 4.13 Menghilangkan Jejak	30
Gambar 4.14 Isolasi Jaringan VM Target	31
Gambar 4.15 Tahap Analisis Network Forensik	31
Gambar 4.16 Record File Flow Log Dalam Bentuk JSON	32
Gambar 4.17 Akuisisi File Flow Logs	32
Gambar 4.18 Tahapan Analisis Virtual Harddisk	33
Gambar 4.19 Pembuatan Snapshot Image	34
Gambar 4.20 Membuat Volume Baru Dari Snapshot Image	35
Gambar 4.21 Attach Volume ke instance	35
Gambar 4.22 Volume Berhasil di-attach	36
Gambar 4.23 Akuisisi Disk Volume	36
Gambar 4.24 Perbandingan checksum	36
Gambar 4.25 Snapshot RAM	37
Gambar 4.26 Owning Memory	37
Gambar 4.27 Hasil Checksum	37
Gambar 4.28 BitQuery GCP	39
Gambar 4.29 Mounting Disk VM Target	40
Gambar 4.30 Membuat File system timeline	40
Gambar 4.31 Testing Plugin Bash	41
Gambar 4.32 Analisis Data Packet Transferred	42
Gambar 4.33 Analisis Data Traffic Port Tertentu	42
Gambar 4.34 Analisis Data Traffic Dari Suspect IP	43
Gambar 4.35 Artefak Filesystem Timeline	45
Gambar 4.36 Bukti Potensial	45
Gambar 4.37 Aktifitas Bruteforce	47
Gambar 4.38 Attacker Membuat User Baru	47
Gambar 4.39 Bukti Adanya Exploit Webmin	48

Gambar 4.40 Service yang berjalan dengan plugin pslist	49
Gambar 4.41 Melihat Perintah Yang Menjalankan Service	49
Gambar 4.42 Cek perintah yang dijalankan melalui bash	50



## DAFTAR LAMBANG DAN SINGKATAN

GCP	Google Cloud Platform
VM	Virtual Machine
NIST	National Institute Of Standards And Technology
VHD	Virtual Harddisk
SSH	Secure Shell
PCAP	Packet Capturing
IOC	Indicator Of Compromise



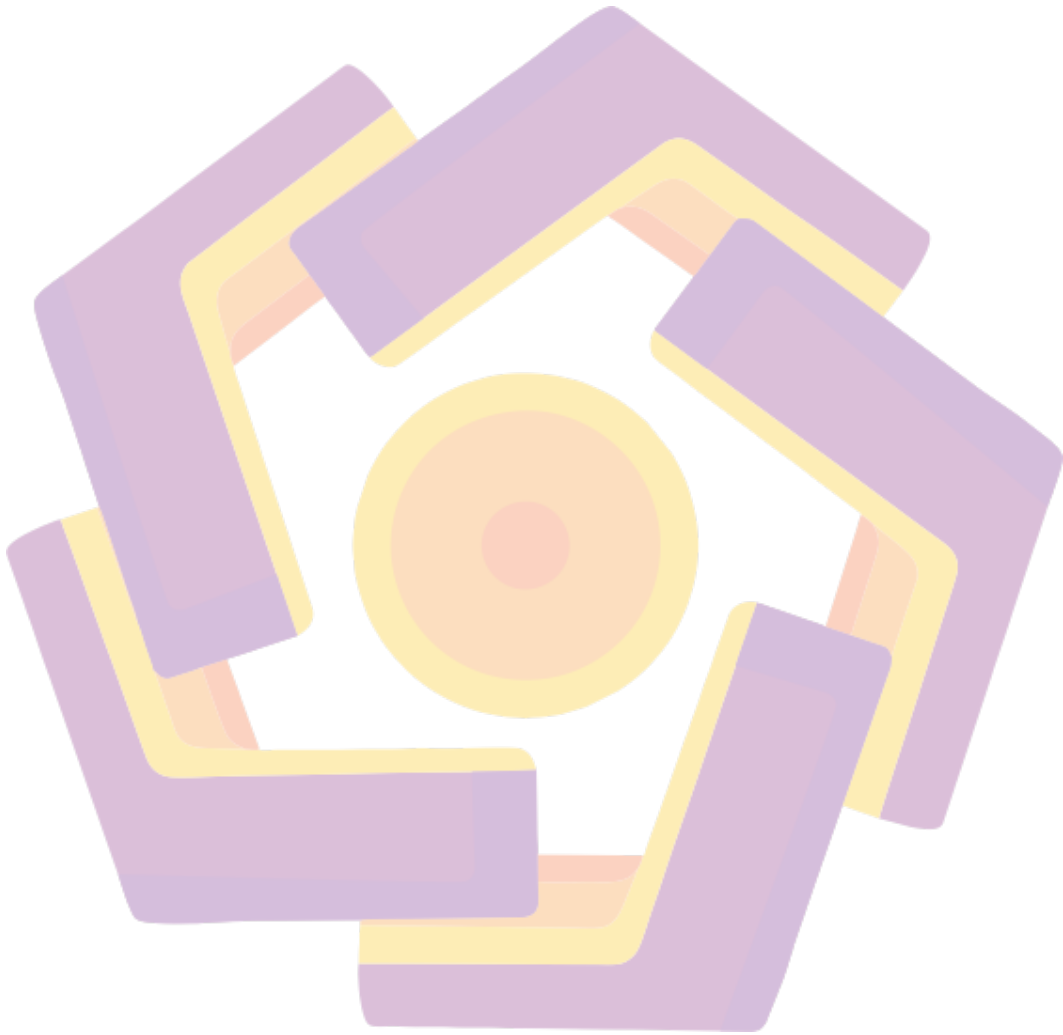
## DAFTAR ISTILAH

Attacker/Threat Actor

Pelaku Penyerangan

Eksaminasi

Tahap Pra-duga





## INTISARI

Implementasi teknologi cloud computing pada berbagai sektor industri dan kebutuhan manusia saat ini sudah sangat populer. Banyak perusahaan besar melakukan migrasi teknologi ke infrastruktur cloud. Cepatnya perkembangan development dari sisi teknologi dan arsitektur cloud computing menjadi tantangan baru pada kasus digital forensik dalam mencari bukti potensial dalam penanganan kasus cybercrime. Proses akuisisi atau data collection pada teknologi cloud banyak memiliki perbedaan dibandingkan arsitektur on-premise karena adanya teknologi baru di belakangnya. Untuk mendukung investigator dalam analisis forensik di sektor cloud, penelitian ini akan membahas proses investigasi barang bukti dengan studi kasus hacking pada VM Google Cloud, yang merupakan layanan infrastructure as a service (IAAS) milik provider Google Cloud menggunakan metodologi National Institute of Standards Technology (NIST). Investigasi barang bukti berdasarkan kombinasi hasil akuisisi data VM image storage dan kombinasi artefak inbound / outbound traffic yang bisa didapat pada layanan VPC Flow Logs.

**Kata kunci:** Incident Response, Digital Forensic, Cloud Forensic, Cloud computing

## ABSTRACT

*The implementation of cloud computing technology in various industrial sectors and human needs is currently very popular. Many large companies are migrating technology to cloud infrastructure. The rapid development in terms of technology and cloud computing architecture is a new challenge in digital forensic cases in finding potential evidence in handling cybercrime cases. The acquisition process or data collection in cloud technology has many differences compared to the on-premise architecture because of the new technology behind it. To support investigators in forensic analysis in the cloud sector, this study will discuss the process of investigating evidence with hacking case studies on Google Cloud VMs, which are infrastructure as a service (IAAS) services owned by Google Cloud providers using the National Institute of Standards Technology (NIST) methodology. ). Investigation of evidence based on a combination of VM image storage data acquisition results and a combination of inbound / outbound traffic artifacts that can be obtained on the VPC Flow Logs service*

**Keyword:** *Incident Response, Digital Forensic, Cloud Forensic, Cloud computing*