Laporan Hasil Investigasi pada Email Spam

Mata Kuliah Digital Forensik

Dosen Pengampu : Deni Suprihadi, S.T, M.Kom., MCE.

Disusun Oleh :

Khairunnisa Dwi W	**20221310070**
Neng Eva Masliah	**20221310079**
Ratna Santika	**20221310081**
Santi Febrianti	**20221310084**

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER DAN SISTEM INFORMASI

UNIVERSITAS KEBANGSAAN REPUBLIK INDONESIA

TAHUN 2025

Form Bukti Digital

EVIDENCE CHAIN OF CUSTODY

Case Number: 01 Offense: Pengiriman email spam yang mengatasnamakan PT Adaro Indonesia

Submitting Officer: (Name/ID#) Tim Investigasi Forensik

Victim: Santi Febrianti

Suspect: Neng Eva M. (menggunakan email nengevam10@gmail.com)

Date/Time Seized 12 Oktober 2025 / 17:55 WIB Location Of Seizure: Gmail (email server)

Description of Evidence

Item #	Quality	Description of Item
Email Spam ('Panggilan Tes Rekrutmen PT Adaro Indonesia')	OK	Email mencurigakan dikirim ke korban menggunakan domain gmail.com
Header Email (209.85.208.45)	OK	Metadata menunjukkan IP pengirim berada di Amerika Serikat (ARIN)
Domain Pengirim (gmail.com)	OK	Domain valid milik Google namun digunakan untuk tindakan penipuan
Alamat Pengirim (nengevam10@gmail.com)	OK	Akun Gmail digunakan untuk menyamar sebagai pihak HR PT Adaro Indonesia
File hasil validasi SPF, DKIM, DMARC	OK	Menunjukkan email lulus autentikasi namun digunakan untuk spam

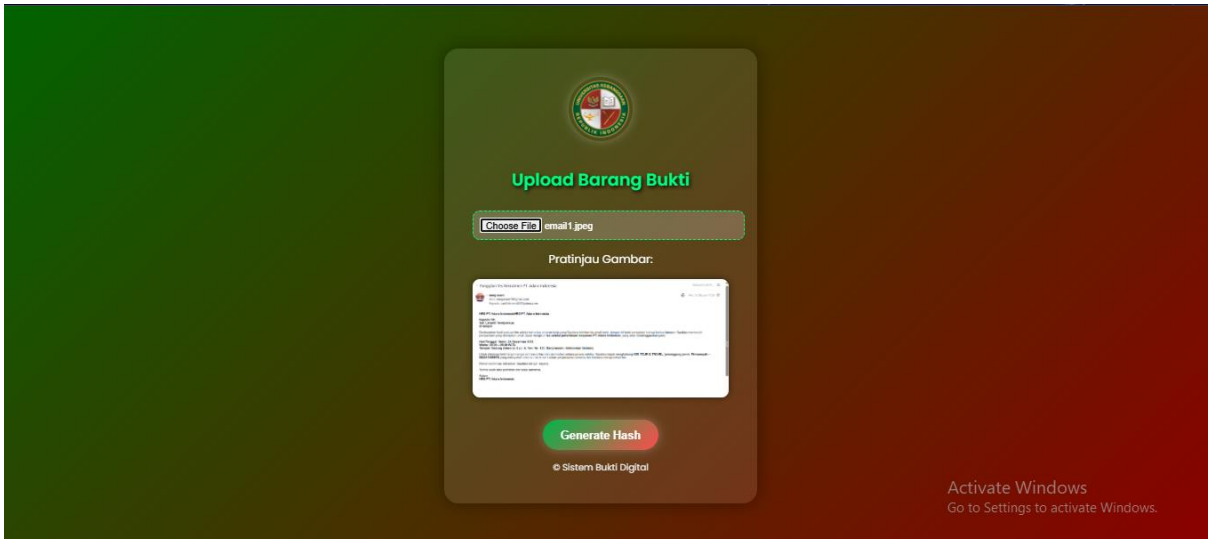
Chain of Custody

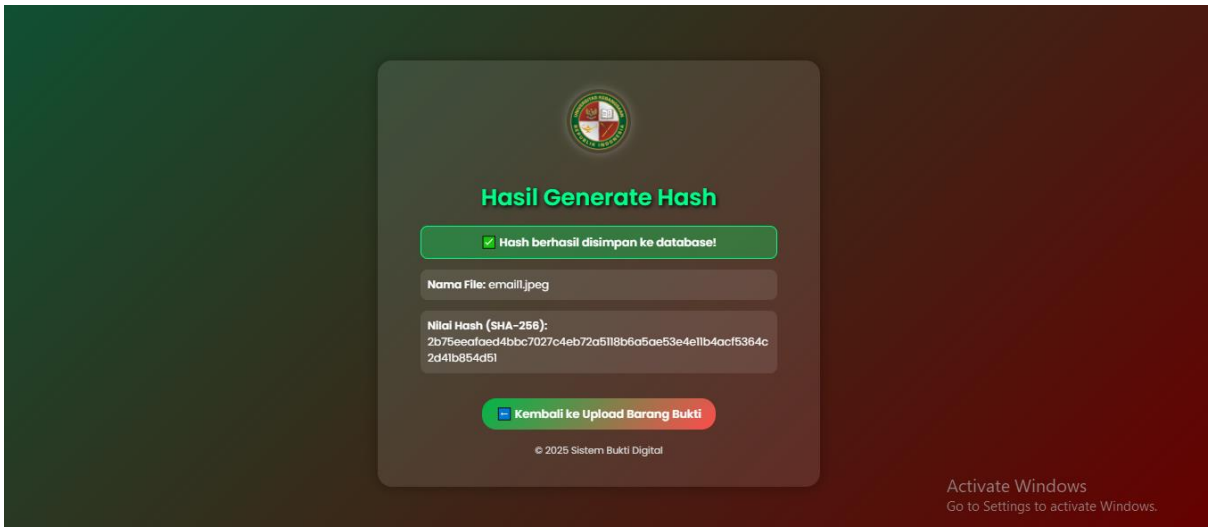
Item #	Date/Time	Received by	Comments/Location
Email Spam	12 Okt 2025	Khairunnisa Dwi W	Diterima dari korban untuk
Header Email	12 Okt 2025	Neng Eva Masliah	Diperiksa untuk identifikasi
Domain Pengirim	12 Okt 2025	Ratna Santika	Diverifikasi melalui validasi domain
Alamat Pengirim	12 Okt 2025	Santi Febrianti	Diverifikasi melalui metadata email
Validasi SPF, DKIM,DMARC	12 Okt 2025	Tim Forensik	Hasil pemeriksaan email header

Kesimpulan

Berdasarkan hasil investigasi digital, email tersebut berasal dari domain gmail.com dan memiliki IP address 209.85.208.45 yang terdaftar di Amerika Serikat. Meskipun autentikasi SPF, DKIM, dan DMARC berstatus PASS, email ini merupakan bentuk penipuan (phishing/spam) karena mencatut nama PT Adaro Indonesia secara tidak sah.

Barang Bukti





Upload Barang Bukti

Choose File header1.jpeg

Pratinjau Gambar:

Generate Hash

© Sistem Bukti Digital

Hasil Generate Hash

✅ Hash berhasil disimpan ke database!

Nama File: header1.jpeg

Nilai Hash (SHA-256):
e53ffbe1b1d2a9e6a9ed9cc85c91bb03bd577bd41f43ff17c2a20271b6e8f313

⬅ Kembali ke Upload Barang Bukti

© 2025 Sistem Bukti Digital

Upload Barang Bukti

Choose File header2.jpeg

Pratinjau Gambar:

Generate Hash

© Sistem Bukti Digital

Hasil Generate Hash

✅ Hash berhasil disimpan ke database!

Nama File: header2.jpeg

Nilai Hash (SHA-256):
018a27df9b38aee6aefa3b731a60bf14640ec09cbf3ff8c6334e98835429e78b

Kembali ke Upload Barang Bukti

Upload Barang Bukti

Choose File header3.jpeg

Pratinjau Gambar:

Generate Hash

Hasil Generate Hash

✅ Hash berhasil disimpan ke database!

Nama File: header3.jpeg

Nilai Hash (SHA-256):
5dc7b9ca822e30cb96fc1e758edc847f383d6f98de670a46066327f5f81fdd22

Kembali ke Upload Barang Bukti

Upload Barang Bukti

Choose File centra1.jpeg

Pratinjau Gambar:

Generate Hash

© Sistem Bukti Digital

Hasil Generate Hash

✅ Hash berhasil disimpan ke database!

Nama File: central1.jpeg

Nilai Hash (SHA-256):
9488f25260b4ef6d5c2507276b12135468e8f15995c82909309583b8c26b97b2

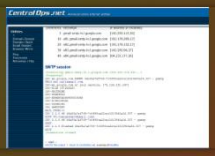
⬅ Kembali ke Upload Barang Bukti

© 2025 Sistem Bukti Digital

Upload Barang Bukti

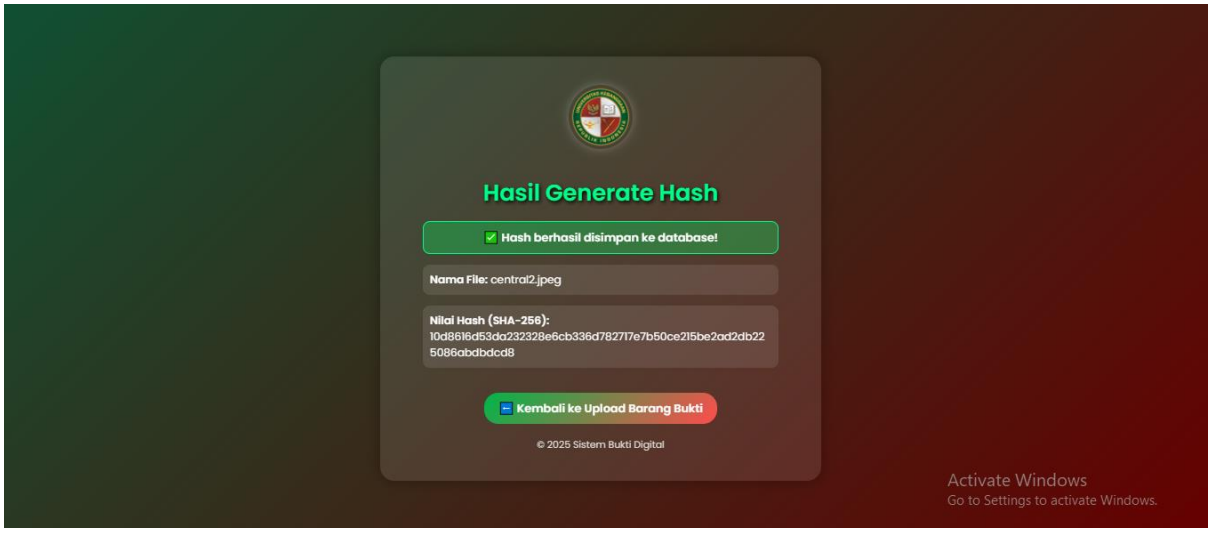
Choose File central2.jpeg

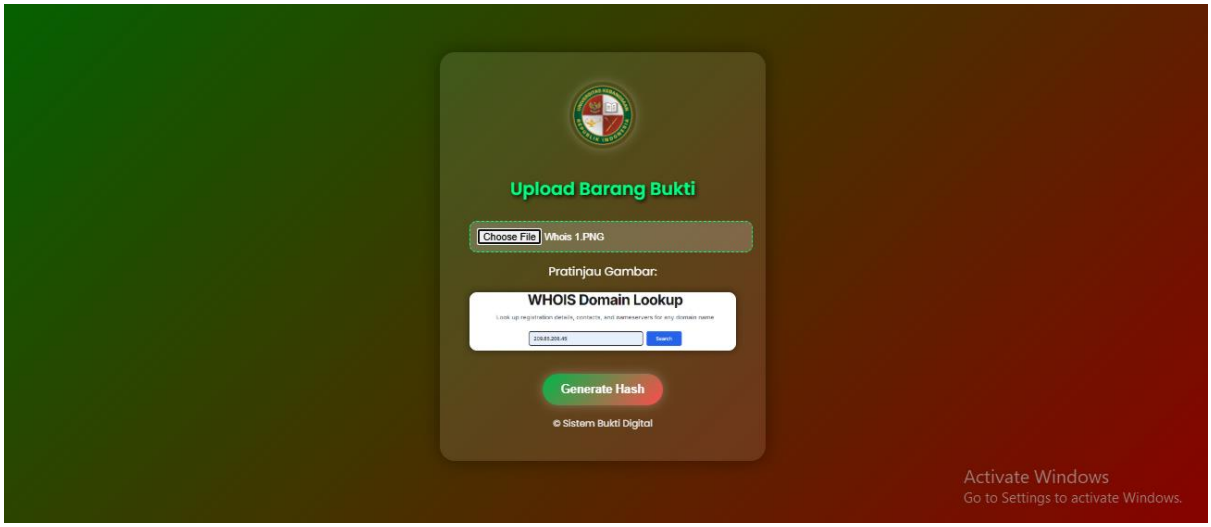
Pratinjau Gambar:

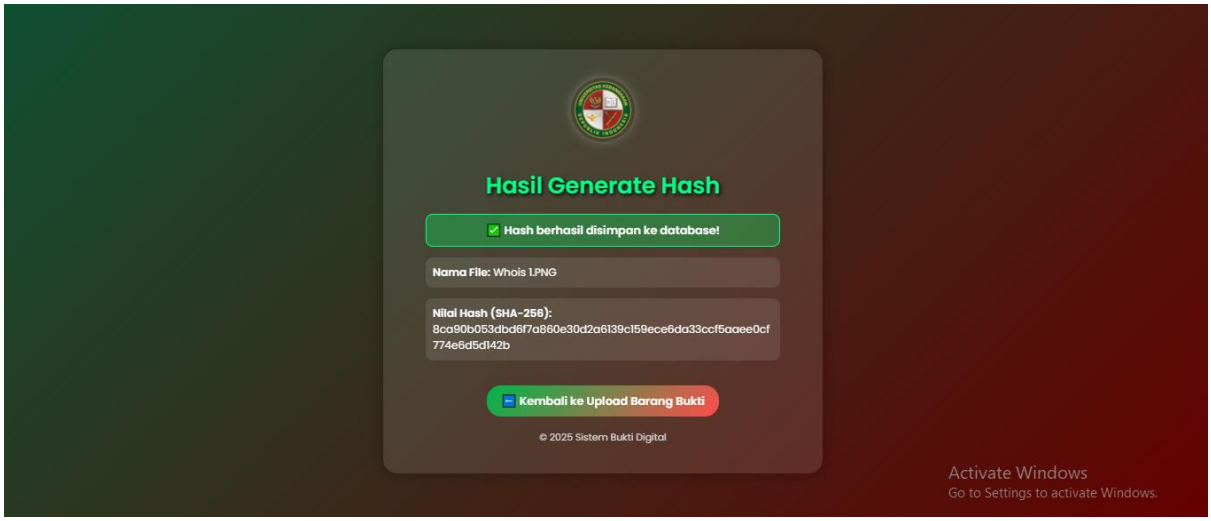


Generate Hash

© Sistem Bukti Digital


Hasil Generate Hash
Hash berhasil disimpan ke database!
Nama File: central2.jpeg
Nilai Hash (SHA-256):
10d8616d53da232328e6cb336d782717e7b50ce215be2ad2db225086abdbdcd8
Kembali ke Upload Barang Bukti
© 2025 Sistem Bukti Digital
Activate Windows
Go to Settings to activate Windows.


Upload Barang Bukti
Choose File
Whois 1.PNG
Pratinjau Gambar:
WHOIS Domain Lookup
Generate Hash
© Sistem Bukti Digital
Activate Windows
Go to Settings to activate Windows.


Hasil Generate Hash
Hash berhasil disimpan ke database!
Nama File: Whois 1.PNG
Nilai Hash (SHA-256):
8ca90b053dbd6f7a860e30d2a6139c159ece6da33ccf5aaee0cf774e6d5d142b
Kembali ke Upload Barang Bukti
© 2025 Sistem Bukti Digital
Activate Windows
Go to Settings to activate Windows.

Upload Barang Bukti

Choose File | Whois 2.PNG

Pratinjau Gambar:

Generate Hash

© Sistem Bukti Digital

Hasil Generate Hash

✅ Hash berhasil disimpan ke database!

Nama File: Whois 2.PNG

Nilai Hash (SHA-256):
023ed3655a041e71c9b4e8cf90640a29ac19ac49cf7c51a102f3a51089b3c77e

Kembali ke Upload Barang Bukti

© 2025 Sistem Bukti Digital

Upload Barang Bukti

Choose File | Wo is 3.PNG

Pratinjau Gambar:

Generate Hash

© Sistem Bukti Digital

Hasil Generate Hash

✅ Hash berhasil disimpan ke database!

Nama File: Wo is 3.PNG

Nilai Hash (SHA-256):
0a188e3322f2c1fa167e373b9651e32f5f616d597cf1fcdd434a3b20d2ce2d34

Kembali ke Upload Barang Bukti

Upload Barang Bukti

Choose File | Toolbox1.PNG

Pratinjau Gambar:

Generate Hash

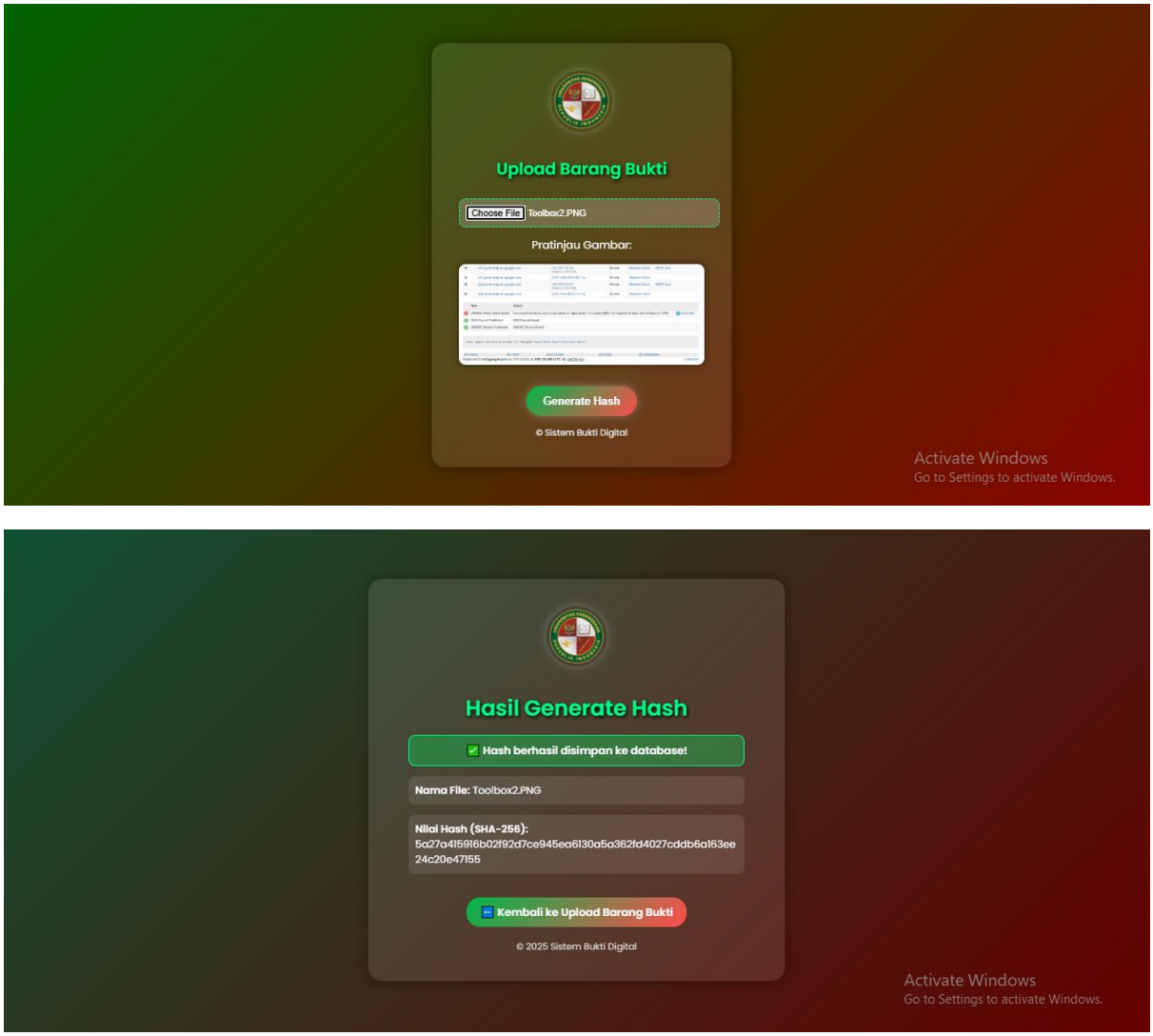
Hasil Generate Hash

✅ Hash berhasil disimpan ke database!

Nama File: Toolbox1.PNG

Nilai Hash (SHA-256):
0a72f5f92d10c4967808d509778786ece3215fb2877a174922d2eb0e32ee2af1

Kembali ke Upload Barang Bukti



SHA-256 Email Spam

Kesimpulan

Barang bukti digital yang telah diupload ke sistem dan diverifikasi menggunakan algoritma hash SHA-256 terbukti valid (sah) dan autentik (asli). Nilai hash menunjukkan bahwa tidak ada perubahan atau manipulasi pada file setelah proses pengumpulan. Oleh karena itu, seluruh barang bukti digital dapat digunakan sebagai bukti sah dalam laporan hasil investigasi kasus email spam.

Tabel Hasil Integrity Bukti

No	Nama Barang Bukti	Nilai SHA-256	Tahapan
1	Pesan Asli Email Spam	2b75eeafaed4bbc7027c4eb72a5118b6a5ae53e4e11b4acf5364c2d41b854d51	Barang Bukti Digital
2	Header Email (Metadata Email)	e53ffbe1b1d2a9e6a9ed9cc85c91bb03bd577bd41f43ff17c2a20271b6e8f313	Securing documentation
3	Header Email (Metadata Email)	018a27df9b38aee6aefa3b731a60bf14640ec09cbf3ff8c6334e98835429e78b	Securing documentation
4	Header Email (Metadata Email)	5dc7b9ca822e30cb96fc1e758edc847f383d6f98de670a46066327f5f81fdd22	Securing documentation
5	Validasi Email (Hasil Pemeriksaan Provider)	9488f25260b4ef6d5c2507276b12135468e8f15995c82909309583b8c26b97b2	Examination poin a
6	Validasi Email (Hasil Pemeriksaan Provider)	10d8616d53da232328e6cb336d782717e7b50ce215be2ad2db225086abdbdcd8	Examination poin a
7	Check IP Address (209.85.208.45)	8ca90b053dbd6f7a860e30d2a6139c159ece6da33ccf5aaee0cf774e6d5d142b	Examination poin b
8	Check IP Address (209.85.208.45)	023ed3655a041e71c9b4e8cf90640a29ac19ac49cf7c51a102f3a51089b3c77e	Examination poin b
9	Check IP Address (209.85.208.45)	0a188e332212c1fa167e373b9651e32f5f616d597cf1fcdd434a3b20d2ce2d34	Examination poin b
10	Kesimpulan Investigasi Email Spam	0a72f5f92d10c4967808d509778786ece3215fb2877a174922d2eb0e32ee2af1	Analysis poin a hasil akhir investigasi email palsu
11	Kesimpulan Investigasi Email Spam	5a27a415916b02f92d7ce945ea6130a5a362fd4027cddb6a163ee24c20e47155	Analysis poin a hasil akhir investigasi email palsu

Dokumen ini merupakan hasil integrasi antara barang bukti digital dan nilai hash (SHA-256) berdasarkan proses investigasi pada kasus Email Spam. Setiap tahapan disusun sesuai urutan proses digital forensik dari akuisisi hingga analisis akhir. Setiap barang bukti digital telah diverifikasi keasliannya menggunakan nilai hash SHA-256, yang menunjukkan bahwa tidak ada modifikasi atau perubahan terhadap data digital asli. Oleh karena itu, hasil investigasi dapat dinyatakan valid dan autentik.

Hasil Investigasi Akun Email Spam

No	Akun Email	Entity	Entity Result	Authenticity (terhadap bukti yang ada)
1	nengevam10@gmail.com	Alamat Email	Domain gmail.com (Google Inc.)	PASS
		Header Email	209.85.208.45 (AS / ARIN)	Valid
		SPF	PASS	Valid
		DKIM	PASS	Valid
		DMARC	PASS	Valid
2	santifebrianti02@yahoo.com	Alamat Email Penerima	Domain yahoo.com	Valid
		Pesan	Subjek: Panggilan Tes Rekrutmen PT Adaro Indonesia	Diduga Palsu
		Isi Pesan	Email mengatasnamakan PT Adaro Indonesia	Tidak valid
		IP Address	209.85.208.45 (wilayah Amerika Serikat / ARIN)	Valid namun disalahgunakan

Kesimpulan

Berdasarkan hasil investigasi digital terhadap email spam yang dikirim oleh akun nengevam10@gmail.com kepada santifebrianti02@yahoo.com, ditemukan bahwa domain pengirim adalah gmail.com milik Google Inc. dan semua validasi autentikasi (SPF, DKIM, DMARC) berstatus PASS. Namun isi pesan mengandung indikasi penipuan karena mencatut nama PT Adaro Indonesia. Alamat IP pengirim (209.85.208.45) terlacak berada di Amerika Serikat dan berada di bawah otoritas ARIN. Sehingga dapat disimpulkan bahwa email tersebut merupakan email spam/phishing.