ANALISIS FORENSIC BERBASIS WEB PHISING MENGGUNAKAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Muhammad Nadhif Hermanto[1], Martanto[2], Iin[3]
STMIK IKMI CIREBON[123]
Jl. Perjuangan No.10B, Karyamulya, Kec. Kesambi, Kota Cirebon, Jawa Barat 45131[123]
E-mail : mnadhifh@gmail.com

ABSTRAK

Menurut Pengelola Nama Domain Internet Indonesia (PANDI) selama lima tahun ke belakangan ada 16.468 laporan phising yang terjadi di domain .id. Untuk penyebaran phising, selain melalui email, pelaku kejahatan menyebarkan alamat link phising menggunakan aplikasi message seperti WhatsApp, Viber, Telegram dan Hangouts. Menurut Kaspersky, dari desember 2020 hingga mei 2021 tercatat sebanyak 91242 kali alamat link phising dibagikan. Di Indonesia terdeteksi ada 738 alamat link phising di WhatApp dan 39 yang dibagikan melalui TelegramUntuk menangkap pelaku phising masih terbentur dengan barang bukti yang wajib di hadirkan dalam persidangan. Bukti tersebut antara lain dapat berupa DNS yang digunakan oleh para phiser (pelaku phising), IP address, hingga identitas penyerang. Tujuan penelitian ini adalah untuk dapat membuktikankejahatan internet berupa barang bukti yang dapat diperoleh dengan menggunakan metode National Institute of Standards and Technology (NIST). MetodeNational Institute of Standards and Technology (NIST) dapat menganalisa proses peninjauan atau jejak digital kasus Kejahatan/penipuan internet dan menampilkan barang bukti digital. Tahapan penelitian ini meliputi collection menggunakan aplikasi Wireshark, examination menggunakan Hashcalc, analisis, dan reporting. Hasil penelitian ini bahwasanya hasil Uji Anova mendapatkan nilai Signifikan sebesar 0.548 > 0.05 yang berarti Teknik dari Metode National Institute Of Standards And Technology Dapat Menganalisis Forensic Berbasis Web Phising.

Kata kunci : Cybercrime, NIST, Phising

ABSTRACTS

According to the Indonesian Internet Domain Name Manager (PANDI) for the past five years there have been 16,468 phishing reports that occurred in the .id domain. For the spread of phishing, other than via email, criminals spread phishing link addresses using messaging applications such as WhatsApp, Viber, Telegram and Hangouts. According to Kaspersky, from December 2020 to May 2021, 91242 phishing link addresses were shared. In Indonesia, it was detected that there were 738 addresses of phishing links on WhatApp and 39 that were shared via Telegram. To catch phishing perpetrators, they still collided with evidence that must be presented in court. This evidence includes the DNS used by phishers (phishers), IP addresses, and the identity of the attacker. The purpose of this study is to be able to prove internet crimes in the form of evidence that can be obtained using the National Institute of Standards and Technology (NIST) method. The National Institute of Standards and Technology (NIST) method can analyze the review process or digital traces of internet crime/fraud cases and display digital evidence. The stages of this research include collection using the Wireshark application, examination using Hashcalc, analysis, and reporting. The results of this study are that the Anova test results get a significant value of 0.548 > 0.05, which means that the technique of the National Institute of Standards and Technology method can analyze web-based forensics for phishing.

Keywords: Cybercrime,NIST,Phising

1. PENDAHULUAN

Situs web phishing ialah suatu web yang dirancang oleh hacker sedemikian rupa supaya menyamai web asli(bentuk, konten, URL daerah ataupun yang lain) buat mencurangi korbannya(konsumen internet) dengan membuat korban seakan lagi mengakses laman web dari pangkal yang legal. Bentuk web hendak terbuat mirip dengan web originalnya supaya korban percaya tengah terletak pada web yang betul. Tidak hanya dari itu, terdapat pula web phising yang dirancang spesial buat membagikan data ataupun petunjuk ilegal yang menyesatkan.(Eka Purwiantono & Tjahyanto, 2017)

Seleksi fitur ialah terkaitnya akrab dengan permasalahan penyusutan ukuran yang mana maksudnya ialah buat menganalisa fitur dalam himpunan informasi- sama berartinya, serta tidak mengikutsertakan fitur lainnya semacam data yang tidak terkait serta dilebih-lebihkan dan akurasi dari seleksinya pada masa depan dapat dikembangkan Pemilahan fitur merupakan satu dari aspek yang sangat berarti yang bisa pengaruhi tingkatan ketepatan pengelompokan sebab bila dataset bermuatan beberapa fitur, format ruang hendak jadi besar serta non- bersih, mengurangkan tingkatan ketepatan pengelompokan Permasalahan dalam pemilahan merupakan penurunan format, dimana awal mulanya seluruh ciri dibutuhkan buat mendapatkan ketepatan yang maksimum. 4 alibi penting buat melaksanakan penurunan.

Peneliti sebelumnya dilakukan oleh Halim, Zuhri yang berjudul "Prediksi Website Pemancing Data Utama Phising Memakai Support Vector Machine (SVM)" Peneliti tersebut mengatakan bahwa riset ini pengarang melakukan percobaab dengan memberi ilustarsi performa perkiraan kepada web phishing memakai tata cara Support Vector Machine setelah itu membandingkan dengan tata cara Naïve Bayes serta Decision Tree, dari analogi itu diinginkan riset ini bisa membagikan cerminan tata cara yang sangat berdaya guna serta cermat dalam memperhitungkan web phishing.(Halim, 2017)

Riset yang dicoba oleh penulis ialah "Analisis Forensic Berbasis Web Phising Menggunakan Metode National Institute Of Standards And Technology"yang menganalisa tentang Web Phising cara analitis ataupun forensik digital permasalahan cybercrime dapat menimbulkan benda fakta digital. tingkatan penelitian ini meliputi collection menggunakan Wireshark, examination menggunakan Hashcalc, analysis, dan reporting.hasil penelitian ini diharapakan dapat diperoleh barang bukti buat mempermudah investigator dalam menganalisa benda fakta digital. Barang bukti yang didapatkan berbentuk URL phishing, DNS yang dipakai oleh pelakon, IP address server, IP address destination, bukti diri penyerbu serta e-mail yang menciptakan data perbuatan kesalahan yang dicoba phiser.

Kajian yang akan saya usulkan adalah "Analisis Forensic Berbasis Web Phising Menggunakan Teknik National Institute Of Standards And Technology" Riset ini menerapkan tata cara analisis forensik pada Web Phising, Metode itu bisa membilai script ataupun memalsukan suatu website dengan protocols HTTPS pada web yang dipakai oleh pelakon phising. Perihal itu buat menarik atensi korban mengakses URL ataupun web para pelakon phising sebarkan lewat email. Protocols HTTPS memiliki keamanan yang besar dengan metode mengenkripsi informasi memakai algortihma dari perihal ini pelakon phising menggunakan keamanan HTTPS buat membuat website phishing serta pula memastikan korban kalau website itu nyaman buat dipakai. Perampokan account berplatform website phishing dengan fake daerah yang dipakai phiser ataupun pelakon, dengan maksud mengutip informasi yang sensitive pada account korban semacam username serta kata sandi.

Tujuan utama dari riset ini adalah memakai tata cara NIST, tata cara ini dipakai dalam menganalisa resiko teknologi data dengan sebagian tahap yang berfungsi berarti dalam pencarian hasil penaksiran dengan cara efisien serta efesien, selain tujuan utama ada pula tujuan yang kedua untuk mengajak masyarakat Indonesia untuk memerangi phishing, PANDI menerangi phishing yang sering terjalin di bidang digital.

Dalam penyusunan skripsi ini alibi pengarang melaksanakan penentuan dari kepala karangan itu guna mengenali yang digunakan oleh penulis dan Untuk mengetahui penyelesaian Menganalisa Web Phising Memakai teknik National Institute Of Standards And Technology, melawan phisher/Pelaku

P-ISSN: 2337-8344
E-ISSN: 2623-1247

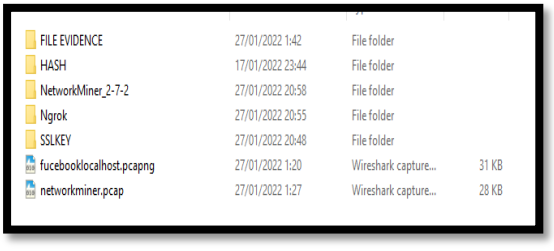
Kejahatan internet amat berarti sebab perkembangan internet yang terus menjadi massif membuat kita butuh tingkatkan kemananan serta daya tahan di internet dari serbuan phishing yang terus menjadi bertambah, Alasan Penulis memilih judul ini ialah menganalisis teknik. Analitis forensik digital mempunyai aplikasi yang amat beraneka ragam. Pemakaian sangat biasa merupakan buat mensupport ataupun melawan anggapan pidana dalam majelis hukum kejahatan ataupun perdata.

2. METODE PENELITIAN

Mempunyai 4 tahapan di dalam metode NIST tersebut:

1. Collection

Pengumpulan informasi memakai tools wireshark buat mengcapture pada dikala korban memperoleh Url link: yang berubah – ubah dikarenakan si pelaku menggunakan jaringan private buat melaksanakan pelayanan perorangan cloud yang gunanya buat mensinkronisasi file, mengirimkan link phising secara aman menggunakan end-to-end encryption, kemudian pelaku menyebarkan link phising dan tanpa sepengetahuan si korban mengakses URL phishing, setelah itu korban login dengan username serta password. File yang tersembunyi didapat buat menolong analitis. Dari kegiatan korban diperoleh file hasil capture(*. pcapng) serta angka hash dari file capture dan diperoleh benda fakta bonus dari berkas SSLKEY serta berkas file bukti



Gambar 1. File Evidence

Gambar diatas menunjukkan 1 file hasil capture(*. pcapng) yang dicoba pada bertepatan pada 27 Januari 2022 dengan file type berbentuk wireshark capture file, berkas file evidence yang bermuatan screenshoot catatan e- mail dari pelakon serta bentuk website phishing, berkas SSLKEY yang bermuatan file batang kayu dari website phishing yang diperoleh dari bertepatan pada 27 Januari 2022 serta didapat pula 1 file bacaan(*. pcap) yang terbuat pada bertepatan pada 27 Januari 2022.
NetworkMiner sebagai tool pendukung dari Wireshark dan sedangkan tools ngrok yaitu untuk mengonversi server localhost yang terdapat ke server masyarakat yang bisa diakses dari mana saja,tools ngrok juga digunakan pelaku untuk bisa diakses oleh si korban

2. Examination

Akuisisi data
Sistem pemerolehan informasi bisa diartikan selaku sesuatu sistem yang berperan buat mengutip, mengakulasi serta mempersiapkan informasi, sampai memprosesnya buat menciptakan informasi yang diinginkan. Tipe dan tata cara yang di seleksi pada biasanya bermaksud buat mempermudah tiap tahap yang dilakukan pada totalitas cara. Tahap akuisisi data menggunakan tools hashcalcs dari setiap Data angka hash dari tiap file di berkas evidence tersembunyi dalam file hash. txt. Angka hash yang terbuat memakai algoritme MD5 dengan tools Hashcalc.

Tabel 2.1 Nilai hash file dari folder

File	Nilai Hash
Foto 1	71b08dcfe6bff4b5dce658584eea009e
Foto 2	b8a4bc74a8eb28cadd1fdca87fcd3c9b
fucebooklocalhost.pcapng	b66731a1f9b1c777643ae862e58feb4b
SSLKEYFILELOG.txt	69d73332913b09df3f2aa4723570363f

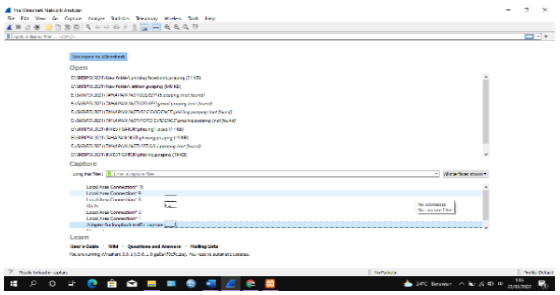
Tahap akuisisi data menggunakan tools hashcalcs dari setiap Data angka hash dari tiap file di berkas evidence tersembunyi dalam file hash. txt. Angka hash yang terbuat memakai algoritme MD5 dengan tools Hashcalc.

3. Analysis

Ada 2 point Pada tahapan Analysis ini mengcapture username dan password milik korban dan filterisasi jaringan, pertama - tama peneliti
menjalankan tools Wireshark untuk mencoba mengcapture username dan password milik korban

P-ISSN: 2337-8344
E-ISSN: 2623-1247

1. Berikut ini adalah langkah – langkah

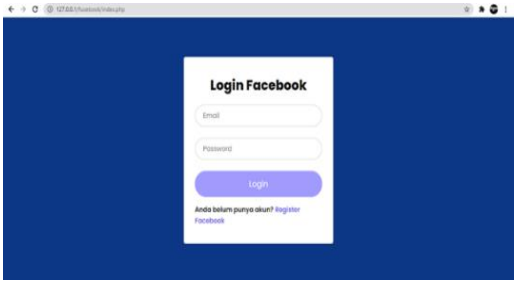


Gambar 2. Tampilan Awal tool Wireshark

2. mengcapture username dan password milik korban, pertama – tama buka tools Wireshark Langkah kedua, buka Google

Gambar 3. Menjalankan Xampp

3. Setelah itu peneliti menajalankan aplikasi Xampp
4. Selanjutnya buka Google Chrome ketikkan "127.0.0.1/fucebook" lalu



Gambar 4. Tampilan Fuceboook

5. Lalu open Wirehark pilih"Adapter for loopback traffic capture" terlihat gambar dibawah ini menunjukkan adanya packet – packet data lalu lintas jaringan

Tabel 2.2 Filterisasi Jaringan

Paket data	Protocol	Dekripsi
Nomor 53	HTTP	GET /fucebook/logout.php
Nomor 77	HTTP	GET / fucebook/biru.jpg
Nomor 79	HTTP	GET /fucebook/style.css
Nomor 142	HTTP	GET /berhasil_login.php

a. Paket data Nomor 53

IP 127.0.0.1 ialah capture isi catatan email URL website phishing yang dikirimkan pelaku pada korban yang dikirimkan bertepatan pada 26 Januari 2022 semacam pada Lukisan dibawah ini.
gambar 5 hasil Capture

b. Paket data Nomor 7

Analysis disektor TCP Wireshark melacak status setiap sesi TCP dan memberikan informasi tambahan ketika masalah atau potensi masalah terdeteksi. Analisis dilakukan sekali untuk setiap paket TCP saat file capture pertama kali dibuka, Paket diproses sesuai urutan kemunculannya dalam daftar paket.

c. Paket data nomor 79

Di Paket data nomor 79 pneliti menambahkan tools pendukung Dari wireshark bernama NetworkMiner, tools pendukung selaku perlengkapan sniffing ataupun perlengkapan buat membekuk informasi informasi paket dalam perihal ini buat mengetahui sistem pembedahan, tahap, julukan Host, port yang terbuka(open Ports), serta mencarifile -file tersembunyi tanpa melimpahkan sedikitpun traffic pada jaringan. NetworkMiner pula bisa menguraikan file PCAP buat di analisa dengan cara off- line, buat mencari file – file tersmbunyi

d. Paket data nomor 142

Pada paket data nomor 79 ditemukannya file tersembunyiPada frame nomor 110 bernama "berhasil_login.php" menunjukkan bahwa

korban tersebut sudah mengakses.

Paket data	Hasil
Paket data Nomor 53	1. Protokol HTTP 2. Url web phising 3. IP Address Source : 127.0.0.1 4. IP Destination : 127.0.0.1 5. Subject : dikirim oleh pelaku pada tanggal 26 januari
Paket data Nomor 77	1. Analisa disektor TCP 2. Initial Round Trip Time (iRTT) 0.0000.98000 sec 3. Bytes in flight: 1181 4. Bytes sent since last PSH Flag: 1181
Paket data Nomor 79	1. Tools : NetworkMiner 2. Struktur – Struktur Project yang digunakan pelaku: Index16.php Index17.php Berhasil_login.php Index18.php
Paket data Nomor 142	1. Subject: 127.0.0.1/fucebook 2. Email korban: hana@gmail.com 3. Password korban: hana123

4. Reporting

tanpa menambahkan sedikit pun traffic pada jaringan. NetworkMiner pula dapat menguraifile PCAP untuk dianalisis dengan metode off-

line,untuk fucebooklocalhost.pcapng diperoleh hasil analisa yang sudah dicoba serta dihidangkan dalam Tabel. Berdasarkan pada Tabel hasil analysis dapat dilihat berbagai informasi seperti alamat IP, identitas penyerang, dan email yang digunakan. Tabel tersebut berisi tentang bukti-bukti dan informasi yang tentang

kejahatan yang dilakukan oleh pelaku. Dapat dilihat pada Tabel tersebut terdapat keanehan data seperti fucebook yang merupakan alamat palsu dari facebook.

3. HASIL DAN PEMBAHASAN

Pada pembahasan ini mengenai uji validitas data dan relibilitas data dari hasil responden terhadap kuisioner yang diberikan. Pengujian ini akan berpengaruh terhadap hasil penelitian berupa Analisis Forensic Berbasis Web Phising memakai Prosedur National Institute Of Standards And Technology

3.1 Hasil Uji Validitas

Uji Validitas Yaitu Uji ketepatan atau ketelitian suatu alat ukur dalam mengukur apa yang sedang ingin diukur. Dalam pengertian yang mudah dipahami, uji validitas adalah uji yang bertujuan untuk menilai apakah seperangkat alat ukur sudah tepat mengukur apa yang seharusnya diukur. Pengujian validitas dilakukan dengan bantuan komputer menggunakan program SPSS for Windows Versi 26. Dalam penelitian ini pengujian validitas hanya dilakukan terhadap15 responden. Pengambilan keputusan berdasarkan pada nilai rhitung (Corrected Item-Total Correlation) > rtabel sebesar 0,514

3.2 Hasil Uji Realibilitas

Uji reliabilitas merupakan alat yang digunakan untuk mengukur konsistensi kuesioner yang merupakan indikator dari variabel atau konstruk. Suatu kuesioner dikatakan reliabel atau handal jika jawaban seseorang terhadap pertanyaan adalah konsisten atau stabil dari waktu ke waktu.

Uji reliabilitas dilakukan terhadap item

pertanyaan yang dinyatakan valid. Suatu variabel dikatakan reliabel atau handal jika jawaban terhadap pertanyaan selalu konsisten. Koefisien reliabilitas instrumen dimaksudkan untuk melihat konsistensi jawaban butir-butir pernyataan yang diberikan oleh responden Adapun alat analisisnya menggunakan metode belah dua (split half) dengan mengkorelasikan total skor ganjil lawan genap, selanjutnya dihitung reliabilitasnya menggunakan rumus "Alpha Cronbach'. Penghitungan dilakukan dengan dibantu komputer program SPSS. Adapun reliabilitas untuk masing-masing variabel hasilnya disajikan pada tabel berikut ini

Tabel 2.3 case P Summary

		N	%
Cases	Valid	14	93.3
	Excluded[a]	1	6.7
	Total	15	100.0

Tabel 6 Realibility Stastics

Cronbach's Alpha	N of Items
.867	

3.3 Hasil Uji Homogenitas

Percobaan homogenitas dipakai buat mengenali apakah sebagian versi populasi merupakan serupa ataupun tidak. Percobaan ini dicoba selaku prasyarat dalam analisa independent sample t test dan Anova. Anggapan yang melandasi dalam analisa versi(Anova) merupakan kalau versi dari populasi adalah serupa. Percobaan kecocokan 2 varians dipakai buat mencoba apakah edaran informasi itu sama ataupun tidak, ialah dengan menyamakan kedua variansnya. Bila 2 golongan data atau lebih memiliki varians yang serupa besarnya, hingga percobaan homogenitas tidak butuh dicoba lagi sebab informasinya telah diduga
Setelah melakukan uji Validitas, maka selanjutnya peneliti melakukan Uji Homogenitas Adapun hasil uji homogenitasnya disajikan pada table ini

Tabel 3.1. Uji Homogenitas

		Levene Statistic	df1	df2	Sig.
Total	Based on Mean	1.005	2	13	.393
	Based on Median	.572	2	13	.578
	Based on Median and with adjusted df	.572	2	11.737	.579
	Based on trimmed mean	.953	2	13	.411

3.4 Uji T/Anova

Setelah melakukan pengujian uji homogenitas penliti melanjutkan pengujian Uji test one way anova
Dasar pengambilan keputusan dalam analisis Anova:

1. Jika nilai Sig > 0.05, Maka Teknik dari Metode National Institute Of Standards And Technology Dapat Menganalisis Forensic Berbasis Web Phising
2. Jika nilai Sig < 0.05, maka dari Metode National Institute Of Standards And Technology tidak Dapat Menganalisis Forensic Berbasis Web Phising

Tabel 3.2. Uji/T Anova

Total

	Sum of Squares	Df	Mean Square	F	Sig.

Butir	Nilai Corrected Item Total Correlation/ R hitung	R Tabel	Kriteria
1	0,773	0,514	Valid
2	0,486	0,514	Tidak Valid
3	0,680	0,514	Valid
4	0,768	0,514	Valid
5	0,661	0,514	Valid
6	0,661	0,514	Valid
7	0,577	0,514	Valid
8	0,674	0,514	Valid
9	0,681	0,514	Valid
10	0,850	0,514	Valid
11	0,467	0,514	Tidak Valid

4. KESIMPULAN

Berikut ini kesimpulan berdasarkan dari Tahapan – Tahapan Metode NIST

Tahapan – Tahapan dari Metode NIST
Riset menciptakan benda fakta dari aplikasi, langkah langkah pada metode National Institute of Standards and Technology (NIST), Tahapan pertama adalah collection (pengumpulan data) dari file capture fucebooklocalhost.pcapng yang didapat dari langkah analysis serangan pada web phishing menggunakan tools Wireshark diberi aplikasi pendukung dari wireshark ialah network miner dan pelaku phising untuk penyebaran linknya menggunakan tools Ngrok. Tahapan kedua adalah examination (akuisisi data) menggunakan Hascalc untuk pemeriksaan nilai hash Message-Digest algortihm 5 (MD5) pada barang bukti digital. Tahapan ketiga adalah analisis pada barang bukti file capture fucebooklocalhost.pcapng yang didapatkan 4 paket informasi yang berkaitan dengan perbuatan kesalahan yang dicoba phiser. Tahapan keempat adalah reporting (pelaporan) melaporkan barang bukti berupa URL phishing, Hasil dari membagi protocols HTTP dengan cara totalitas dengan mendekripsikan bentuk kemudian rute pada protocols TLSv 1. 2 buat mempermudah investigator dalam menganalisa benda fakta digital. Pada dikala analisis ditemui antara buat mendekripsikan protocols HTTP yang dipakai web phishing. Hasil riset ini menunjukkan

Between Groups	51.571	2	25.785	.630	.548
Within Groups	531.867	13	40.913		
Total	583.438	15			

dengan memakai prosedur NIST dapat diperoleh barang bukti berupa informasi yang dipakai oleh pelaku buat melaksanakan kejahatan.

e. Hasil pengujian hipotesis dengan uji Anova Signifikan kerena nilai Sig. untuk faktor sebesar 0.548 > 0.05 yang berarti dapat menganalisis Web Phising Berbasis Metode National Institute Of Standards And Technology

DAFTAR PUSTAKA

[1]. Bintang, R. A., Umar, R., & Yudhana, A. (2020). Analisis Media Sosial Facebook Lite dengan tools Forensik menggunakan Metode NIST. *Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto)*, *21*(2), 125. https://doi.org/10.30595/techno.v21i2.8494

[2]. Eka Purwiantono, F., & Tjahyanto, A. (2017). *Model Klasifikasi Untuk Deteksi Situs Phising Di Indonesia*. 156. https://doi.org/10.13140/RG.2.2.29627.52003

[3]. Elanda, A., & Buana, R. L. (2021). Analisis Manajemen Risiko Infrastruktur Dengan Metode NIST (National Institute of Standards and Technology) SP 800-30 (Studi Kasus : STMIK Rosma). *Elkom : Jurnal Elektronika Dan Komputer*, *14*(1), 141–151. https://doi.org/10.51903/elkom.v14i1.387

[4]. Halim, Z. (2017). Prediksi Website Pemancing Informasi Penting Phising Menggunakan Support Vector Machine (SVM).

Information System for Educators and Professionals, *2*(1), 71–82. http://download.portalgaruda.org/article.php?article=535068&val=10928&title= Prediksi Website Pemancing Informasi Penting Phising Menggunakan Support Vector Machine (SVM)

[5]. Imam Riadi, Abdul Fadlil, & Muhammad Immawan Aulia. (2020). Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST). Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 4(5), 820–828. https://doi.org/10.29207/resti.v4i5.2224

[6]. Nist, A., Dan, S. R. M., Dengan, S. R. M., M, T. R., Yusuf, S., Bahan, P., & Ptbin, N. (n.d.). *Analisis nist srm 1633b dan srm 1646a dengan metode aan dalam rangka ujibanding antar laboratorium*. 149–160.

[7]. Nofiyan, A., & Mushlihudin, M. (2020). Analisis Forensik pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST). *JSTIE (Jurnal Sarjana Teknik Informatika) (E-Journal)*, *8*(2), 53. https://doi.org/10.12928/jstie.v8i2.16697

[8]. Purhanta. (2010). PENGUMPULAN DATA DAN INSTRUMEN PENELITIAN Penelitian. *Http://Etheses.Uin-Malang.Ac.Id/1670/7/11510004_Bab_3.Pdf*, 1–7.

[9]. Raco, J. (2018). *Metode penelitian kualitatif: jenis, karakteristik dan keunggulannya*. https://doi.org/10.31219/osf.io/mzuj

[10]. Riadi, I., & Umar, R. (2017). Identification Of Digital Evidence On Android ' s. *International Journal of Computer Science and Information Security*, *15*(5), 3–8.