KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR (UNM)
LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT
Menara Pinisi Lantai 10 Jalan Andi Pangeran Pettarani Makassar
Telpon (0411) 865677, Fax(0411) 861377 Kode Pos 90222
Laman: www.unm.ac.id email: lppm@unm.ac.id & lemlitunm@yahoo.co.id

SURAT KETERANGAN

Nomor:3940/UN36.11/LP2M/2022

Yang bertanda tangan di bawah ini,

Nama : Prof. Dr. Ir. H. Bakhrani A. Rauf, M.T., IPU.

NIP : 19611016198803 1 006

Jabatan : Ketua Lembaga Penelitian dan Pengabdian Kepada Masyarakat UNM

Dengan ini menerangkan bahwa,

Nama : Drs. Ir. Faisal Syafar, M.Si., M.Inf.Tech., Ph.D., IPU.

NIP : 196509101991031003

Fakultas : FT UNM

Benar telah melaksanakan penelitian dengan judul:

"Deteksi Cepat Wi-fi Evil Twin Attack Menggunakan Metode Live Computer Forensic"

Penelitian ini dilaksanakan selama 7 bulan (Mei s.d. November 2022)

Skema Penelitian: Penelitian PNBP FT UNM Tahun Anggaran 2022

Anggota Peneliti : Misita Anwar, B.Eng., M.InfSc, Ph.D. & Dr. Ir. Muh. Ma`ruf Idris, S.T., M.T., M.M., IPM.

Demikian surat keterangan dibuat untuk dipergunakan sebagaimana mestinya.

Makassar, 30 November 2022
Ketua

Prof. Dr. Ir. H. Bakhrani A. Rauf, M.T., IPU.
NIP 19611016198803 1 006

LAPORAN AKHIR PENELITIAN
PNBP FAKULTAS TEKNIK

DETEKSI CEPAT WI-FI EVIL TWIN ATTACK MENGGUNAKAN METODE LIVE COMPUTER FORENSIC

Ketua/Anggota Tim

Drs. Ir. Faisal Syafar, M.Si., M.InfTech., Ph.D., IPU. /NIDN 0010096503
Misita Anwar, B.Eng., M.InfSc., Ph.D. /NIDN 0022017405
Dr. Muhammad Ma'ruf Idris, ST., MT. /NIDN 0012127103

Dibiayai oleh:
DIPA Universitas Negeri Makassar
Nomor: SP DIPA - 023.17.2.677523/2022, tanggal 27 Juli 2022
Sesuai Surat Keputusan Rektor Universitas Negeri Makassar
Nomor: 595/UN36/HK/2022, tanggal 14 April 2022

UNIVERSITAS NEGERI MAKASSAR

NOVEMBER 2022

HALAMAN PENGESAHAN

Judul Penelitian : Deteksi Cepat Wi-Fi Evil Twin Attack Menggunakan Metode Live Computer Forensic

Ketua Peneliti:

a. Nama Lengkap : Drs. Ir. Faisal Syafar, M.Si., M.InfTech., Ph.D., IPU.
b. NIP/NIDN : 196509101991031003/0010096503
c. Jabatan Fungsional : Lektor Kepala
d. Program Studi : Pendidikan Teknik Elektronika
e. Nomor HP : 081237268675
f. E-mail : faisal.syafar@unm.ac.id

Anggota Peneliti

a. Nama Lengkap : Misita Anwar, B.Eng., M.InfSc, Ph.D.
b. NIP/NIDN : 197401222000032001/0022017405
c. Perguruan Tinggi : Universitas Negeri Makassar
a. Nama Lengkap : Dr. Ir. Muhammad Ma'ruf Idris, ST., MT., M.M., IPM.
b. NIP/NIDN : 197112121997021001/0012127103
c. Perguruan Tinggi : Universitas Negeri Makassar

Lama Penelitian : 8 bulan
Biaya Penelitian yang diusulkan : Rp. 37.000.000,(Tigapuluh Tujuh juta rupiah)
Biaya Penelitian yang disetujui : Rp. 35.000.000 (Tigapuluh Lima Juta Rupiah)
Jumlah Mahasiswa yang Dilibatkan: 2 orang

Makassar, 17 November 2022

Mengetahui,
Dekan FT UNM

Prof. Dr.Ir.H.Muhammad Yahya, M.Kes, M.Eng. IPU., ASEAN Eng.
NIP. 196306231991031002

Ketua Peneliti,

Drs. Ir. Faisal Syafar, M.Si., M.InfTech, Ph.D.IPU
NIP. 196509101991031003

Menyetujui,
Ketua Lembaga Penelitian dan Pengabdian kepada Masyarakat UNM

Prof. Dr. Ir. H. Bakhrani A. Rauf, M.T., IPU.
NIP. 196110161988031006

ABSTRAK

DETEKSI CEPAT WI-FI EVIL TWIN ATTACK MENGGUNAKAN METODE LIVE COMPUTER FORENSIC

Seragan Evil Twin menjadi suatu ancaman yang berbahaya bagi para pengguna jaringan *Wifi*. Pelaku penyerangan ini memanfaatkan AP (*access point*) palsu dengan setingan *gateway* yang berbeda dengan *legitimate* AP, sehingga jenis serangan ini menjadi cukup sulit untuk dideteksi. Proses pengungkapan kasus serangan *MITM based Evil Twin* hanya sebatas mendeteksi aktivitas serangan dan belum ada pembahasan lebih lanjut terkait digital forensik, hal ini di sebabkan karena masih kurangnya SOP (*standart operational Procedure*) dalam menangani kasus ini. Penelitian ini dilakukan dengan tujuan untuk membuat suatu model forensik berdasarkan tahapan analisa dalam kasus *MITM based Evil Twin*. Proses dalam investigasi *MITM based Evil Twin* dilakukan dengan menggunakan metode *live* forensik berbasis *user side*, kemudian dibagi kedalam dua fokus penelitian yaitu, proses analisa *Wifi scanning* untuk melakukan investigasi serangan *Evil Twin* dengan menganalisa atribut maupun kegitan-kegitan yang mencurigakan lainya. Analisa investigasi serangan *MITM* dilakukan dengan menganalisa *network traffic* dalam *area Evil Twin*. Hasil investigasi forensik dalam penelitian, menghasilkan suatu model investigasi ENFGP (*Extendend* NFGP) yang dibagi menjadi 10 tahapan dan terdiri atas 30 langkah – langkah penyelesaian, yang didapatkan melalui proses pengujian dan implenmentasi metode pada kasus serangan *MITM Based Evil Twin* serta pengujian lebih lanjut berdasarkan beberapa model forensik sebelumnya.

Kata kunci: Evil twin attack, Wi-Fi, Live forensic

DAFTAR ISI