Analisis Pengaruh Capture The Flag Jeopardy-Style Dalam Memperkenalkan Pendidikan Digital Forensik Menggunakan Metode User Experience Questionnaire

Mudjrika Meirasari*, Dodi Prima Resda*, Antoni Haikal*

* Politeknik Negeri Batam
Rekayasa Keamanan Siber
Jl. Ahmad Yani, Batam Centre, Batam 29461, Indonesia
E-mail: mudjrika@gmail.com, dodi.prima@polibatam.ac.id, antoni@polibatam.ac.id

Abstrak

Pentingnya pendidikan mengenai keamanan siber di era digitalisasi menjadi hal utama yang harus diperhatikan. Salah satunya melalui konsep gamifikasi yaitu teknik bermain *game* dengan menerapkan aspek pendidikan. Berdasarkan hal ini, *Capture The Flag (CTF)* digunakan sebagai serangkaian tantangan untuk meningkatkan dasar keamanan siber yang meliputi beberapa soal dengan tujuan utama menemukan *flag*. CTF memiliki beberapa bidang, salah satu yang akan dibahas secara spesifik pada paper ini mengenai platform *CTF Jeopardy-Style* khusunya digital forensik yang telah dibuat untuk memperkenalkan pendidikan digital forensik khusunya pemula. digital forensik digunakan untuk mengidentifikasi dan melakukan analisis terkait bukti digital. Dalam konteks CTF, peserta diminta untuk mengumpulkan informasi, menganalisis file, dan memecahkan tantangan soal menggunakan teknik digital forensik, baik menggunakan *tool* atau secara manual, untuk mendapatkan *flag* sebagai bukti keberhasilan menyelesaikan tantangan. Keterkaitan antara CTF dan digital forensik memberikan landasan penting dalam pengembangan keahlian yang diperlukan dalam melawan kejahatan digital. Dengan tambahan penggunaan UEQ sebagai alat bantu untuk dilakukannya pengujian platform pembelajaran yang telah dibuat, dinilai sudah memenuhi ekspetasi pengguna atau belum berdasarkan pengalaman mereka saat bermain.

Kata kunci: Gamifikasi, CTF, Flag, Digital Forensik, Keamanan Siber, UEQ

Abstract

The importance of cybersecurity education in the digitalization era is a big concern. One of them is through the concept of gamification, which is a technique of using games by applying educational principles. Based on this, Capture The Flag (CTF) is used as a set of challenges to improve the basics of cybersecurity which includes several questions with the primary goal of finding the flag. CTF has several fields, one of which will be discussed specifically in this paper regarding the CTF Jeopardy-Style platform especially digital forensics which has been created to introduce digital forensics education especially for beginners. digital forensics is used to identify and analyze digital evidence. In the concept of CTF, participants are required to gather information, analyze files, and solve the challenge of the question using digital forensic techniques, either using tools or manually, to get flags as evidence of successful completion of the challenge. The interrelation between CTF and digital forensics provides an important foundation in the development of skills needed to fight digital crime. Additionally, UEQ is used as a tool to test the learning platform to determine if it is fulfilling the user's expectations based on their experience while playing.

Keywords: Gamification, CTF, Flag, Digital Forensic, Cyber Security, UEQ

1. Pendahuluan

Seiring dengan meningkatnya kejahatan dalam dunia digital, permintaaan akan tenaga professional bidang keamanan siber semakin dibutuhkan[1]. Berbagai institusi pendidikan, organisasi pemerintah, dan juga perusahaan swasta menyadari hal ini, sehingga memperkenalkan konsep pendidikan melalui jalur informal yang lebih efektif dan menyenangkan[2], [3]. Melalui konsep gamifikasi, *Capture The Flag (CTF)* merupakan serangkaian tantangan dalam meningkatkan dasar-dasar keamanan siber dengan tujuan menemukan *flag* pada soal yang telah ditentukan[4]. Setiap soal memiliki beberapa celah kerentanan keamanan yang harus dieksploitasi atau diselesaikan, tingkatan kemudahan dan kesulitan soal tergantung poin-poin yang tertera pada setiap soal[5]. Kompetisi CTF telah diadakan secara online dan offline sejak tahun 1996[6]. Sejak kompetisi ini diperkenalkan, beberapa kompetisi telah memberikan hasil yang signifikan dalam meningkatkan minat siswa terhadap keamanan siber[7].

CTF terbagi menjadi dua tipe yaitu *Jeopardy-Style* dan *Attack and Defense*[8]. *Jeopardy-Style* memiliki beberapa bidang seperti *cryptography*, *web exploit*, *osint*, *digital forensic*, PWN, dan *reverse engginering*[8]. Sedangkan *Attack and Defense* yaitu penyerangan terhadap server tim lawan dan menjaga server sendiri agar tidak diserang oleh pihak lawan[8]. Pada paper ini akan dibahas secara spesifik mengenai analisis pengaruh *Capture The Flag Jeopardy-Style* dalam memperkenalkan pendidikan digital forensik dengan menggunakan *User Experience Questionnaire (UEQ)*.

Digital Forensik menjadi ilmu penting yang tidak hanya digunakan dalam proses investigasi, namun juga dibutuhkan ketika terjadinya suatu insiden seperti manipulasi data digital, peretasan situs hingga kasus terorisme[9]. Seorang investigator harus memiliki pengetahuan tentang penggunaan *tools* atau alat digital forensik, dan memahami suatu insiden yang akan diidentifikasi, serta respon apa yang akan dilakukan setelahnya. Beberapa tugas mereka secara umum adalah untuk menjaga, menemukan, mengontrol, dan memperbaiki setiap insiden yang terjadi[10]. Dalam pembelajaran melalui CTF, digital forensik dan steganografi saling berkaitan. Steganografi dapat dikatakan sebagai teknik penyembunyian pesan dalam sumber daya digital, seperti teks, gambar, audio, video dan bahkan jaringan[11]. Digital Forensik pada soal CTF, biasanya menggunakan teknik steganografi di awalannya, agar peserta terkecoh terhadap data yang ada.

Dengan Memahami penggunaan teknik steganografi, dapat membantu dalam melakukan analisis digital forensik. Peserta CTF dapat lebih efektif dalam melakukan analisis digital forensik. Mereka akan didorong untuk mengumpulkan informasi, menganalisis file, dan memecahkan tantangan soal yang telah diberikan baik menggunakan *tool* atau secara manual. Kemudian mendapatkan *flag* yang akan menjadi bukti keberhasilan dalam menyelesaikan tantangan tersebut. Keterkaitan antara CTF dan digital forensik memberikan landasan penting dalam pengembangan keahlian yang diperlukan dalam melawan kejahatan digital[12].

Penggunaan analisis user experience dilakukan untuk menguji apakah produk yang diciptakan sudah memenuhi ekspetasi dari pengguna atau belum dan apakah diperlukannya perbaikan dari produk tersebut untuk hasil yang lebih memuaskan. Dengan adanya UEQ dan uji regresi dapat menjadi jawaban dari pengujian tersebut. Terdapat beberapa faktor yang memengaruhi pengisian kuesioner oleh responden, termasuk sikap netral yang menyebabkan kebingungan dan kejenuhan dalam menjawab setiap pertanyaan. Diperlukan penyesuaian dalam menyusun tiap pertanyaan dalam kuesioner, dengan mempertimbangkan skala dari setiap pertanyaan berdasarkan formulir UEQ[13].

2. Studi Pendahuluan

Pada beberapa penelitian sebelumnya, telah diamati mengenai berbagai pengaruh CTF dalam dunia pendidikan keamanan siber, salah satunya dalam bidang digital forensik. penelitian terkait telah menyoroti efek positif CTF dalam membangkitkan minat siswa yang mungkin tidak memiliki latar belakang teknis sebelumnya. Penulis menekankan bahwa CTF dapat memberikan dorongan kepada peserta dengan teknik gamifikasi, memperkenalkan dasar-dasar digital forensik melalui platform kompetensi yang ramah pemula. Tantangan yang diajukan, seperti membaca dan menganalisis skenario digital forensik, tidak hanya membangun keterampilan, tetapi juga memperkenalkan konsep steganografi dan stegaanalisis, meningkatkan pemahaman peserta tentang keamanan siber dan peluang karir di bidang tersebut [12].

Di sisi lain, penelitian lainnya juga menunjukkan bahwa kombinasi minat terhadap video game dan teknik gamifikasi membuat pembelajaran menjadi lebih mudah, menyenangkan, dan membuat siswa terlibat secara lebih intensif. Ada berbagai platform online dan komunitas yang didedikasikan untuk pendidikan keamanan siber, dan beberapa situs web menawarkan jalur pembelajaran mandiri untuk mengajarkan forensik dan banyak topik lainnya. Meskipun demikian, penelitian ini menekankan kebutuhan untuk merancang kompetensi secara internal dengan menggunakan teori gamifikasi, menggantikan model kelas tradisional dengan sistem penilaian berbasis poin dari capaian soal yang berhasil dikerjakan [14].

Pembahasan mengenai dampak positif CTF terhadap hasil pembelajaran meningkat secara statistik dan pemahaman tentang keamanan siber termasuk digital forensik yang menjadi bagian dari yang diperlombakan. Terdapat juga tantangan sehingga diperlukan pengetahuan yang baik bagi penyelenggara dan peserta untuk mengorganisir kompetensi CTF yang sangat kompleks. Tantangan lainnya terkait Implikasi etis dari pengajaran metode keamanan komputer yang ofensif, menyebabkan siswa membagikan flag secara ilegal[15].

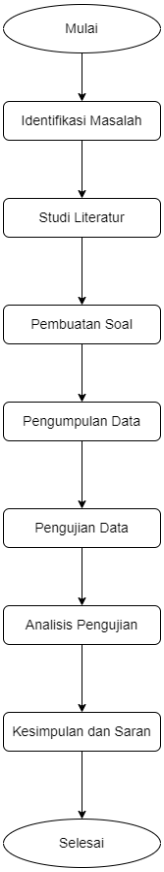
Penelitian lainnya juga membahas bahwa keberhasilan CTF dapat dipengaruhi oleh faktor-faktor seperti tingkat pengalaman peserta. Oleh karena itu, perhatian cermat terhadap dinamika kompetensi dan upaya untuk mengatasi tantangan yang mungkin muncul dianggap kunci untuk memastikan kelancaran pelaksanaan CTF dan maksimalkan manfaatnya bagi peserta. Selain itu, pengembangan keterampilan di bidang keamanan siber juga menjadi fokus utama. Latihan-latihan dan kompetisi CTF dirancang untuk meningkatkan kompetensi siswa dalam berbagai aspek keamanan siber, termasuk digital forensik. Penelitian ini menyoroti bahwa tingkat kesulitan latihan memainkan peran penting dalam pengembangan keterampilan tersebut. Dengan adanya kategorisasi tingkat kesulitan (mudah, sedang, dan sulit), para siswa dapat berkembang secara progresif, memperoleh keterampilan dasar terlebih dahulu sebelum menantang diri mereka dengan tugas yang lebih kompleks [7].

Peneliti mencatat bahwa kompetisi CTF membuka peluang untuk mengembangkan keterampilan forensik yang kritis dalam mendeteksi dan menanggapi ancaman keamanan. Para peserta didik dapat mengasah kemampuan dalam mengekstraksi informasi berbahaya, menyematkan kode tersembunyi, dan melacak jejak penyerang dalam jaringan. Penelitian ini berfokus pada evaluasi efisiensi pengembangan keterampilan ini di kalangan peserta kompetisi CTF, menggambarkan bagaimana peserta yang telah berkembang secara profesional dilengkapi dengan keterampilan yang diperlukan untuk menghadapi tantangan di dunia keamanan siber [7]. Selain itu, pentingnya fitur dari platform CTF dapat mempengaruhi peningkatan proses pembelajaran. Aspek pentingnya dengan ada penambahan alur cerita dalam soal juga menambah pemikiran kritis dari tiap peserta dalam menganalisis soal [16].

Dalam literatur terkait, pentingnya umpan balik pengguna terhadap produk atau layanan telah menjadi fokus utama penelitian[17]. UEQ telah diakui sebagai alat yang efektif untuk mengumpulkan data survei yang berkaitan dengan pengalaman pengguna. UEQ dirancang untuk menghasilkan tanggapan pengguna dengan cepat, sehingga mereka dapat mengekspresikan perasaan, kesan, dan sikap mereka terhadap suatu produk atau layanan dengan mudah[18]. Sedangkan uji regresi dilakukan untuk membantu mengidentifikasi atau memprediksi terkait pengalaman pengguna terhadap produk yang diciptakan, sehingga dapat memberikan informasi untuk membantu dalam meningkatkan produk tersebut[19].

3. Metode Penelitian

Penelitian ini dilakukana dengan membuat soal digital forensik pada platform HarisCTF. Kemudian diuji pengalaman pengguna menggunakan User Experience Questionnaire. Penyebaran kusioner melalui Google Form untuk mendapatkan jawaban dari responden. Alur penelitiannya sebagai berikut.



Gambar 1: Alur Penelitian

Penelitian ini dimulai dengan identifikasi masalah untuk memperoleh topik apa yang akan diambil. Dilanjutkan studi literatur untuk pembahasan terkait teori yang berhubungan dengan topik penelitian, guna mendukung penelitian. Setelah itu, melakukan pembuatan soal dan pengumpulan data yang diperoleh dari kusioner, terhadap pengalaman mereka mengerjakan soal tersebut. Kemudian melakukan analisis pengujian menggunakan UEQ dan regresi linear. Pada UEQ, penggunaan *Data Analysis Tools (DAT)* digunakan sebagai alat bantu dalam mengolah data yang diperoleh berdasarkan pengalaman user. Selanjutnya melakukan uji regresi linear untuk memprediksi terkait hubungan antara variabel X dan variabel Y.

3.1 Data Sampling

Dalam penelitian ini, menggunakan responden yang merupakan mahasiswa Politeknik Negeri Batam yang mempunyai pengalaman dalam bermain *CTF Jeopardy-Style* dibidang digital forensik melalui platform HarisCTF dengan jumlah 100 responden. Teknik sampel pada penelitian ini menggunakan sampling jenuh, yaitu menggunakan seluruh responden dalam penelitian.

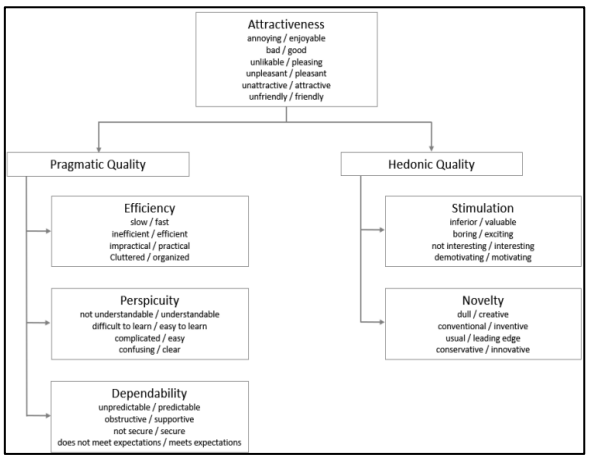
3.2 Variabel Penelitian

Variabel yang digunakan dalam penelitian ini ada dua yaitu variabel X (variabel bebas) dan variabel Y (variabel terikat)[20]. Penjelasannya sebagai berikut:

- Variabel X *(independent variable)*
  Variabel X atau bebas adalah variabel yang mempengaruhi variabel lain[20]. Variabel X pada penelitian ini adalah pengaruh *Capture The Flag Jeopardy-Style* berdasarkan enam indikator yang diuji yaitu *attractiviness, perspicuity, efficiency, dependability, stimulation, novelty*.
- Variabel Y *(dependent variable)*
  Variabel Y atau terikat adalah variabel yang dapat dipengaruhi oleh variabel lain[20]. Variabel Y pada penelitian ini adalah pendidikan digital forensik.

3.3 Instrumen Pertanyaan

UEQ memiliki sejumlah pertanyaan penelitian yang berbeda dan dapat dijawab melalui pengukuran kuantitatif. Semua informasi terkait UEQ diambil dari sumber *(https://www.ueq-online.org/).* Berikut gambar dari pengelompokkan pertanyaan pada UEQ.



Gambar 2: Instrumen Pertanyaan

Terdapat tiga aspek utama, yaitu *Attractiveness, Pragmatic Quality*, dan *Hedonic Quality* dengan enam skala dan 26 item. Setiap skala menggambarkan aspek kualitas yang berbeda. Penjelasan tiap skala yang digunakan sebagai penelitian:

- *Attractiviness* (daya tarik): Kesan terhadap pengalaman peserta dalam bermain CTF Jeopardy-Style dibidang digital forensik.
- *Efficiency* (efisiensi): Kemampuan Peserta CTF *Jeopardy-Style* dalam menyeselaikan tantangan dibidang digital forensik. secara mandiri dan kecepatan mereka dalam menjawab soal, mengikuti petunjuk yang telah diberikan.
- *Perspicuity* (kejelasan): Peserta tidak merasa kebingungan saat menyelesaikan soal CTF *Jeopardy-Style* dibidang digital forensik dengan mengikuti intruksi dan alur yang telah disediakan.
- *Dependability* (ketepatan): Kontrol interaksi peserta dalam mengandalkan rekan tim, ketika bermain CTF *Jeopardy-Style* dibidang digital forensik.
- *Stimulation* (stimulasi): Tingkat kesenangan dan motivasi peserta ketika bermain CTF *Jeopardy-Style* dibidang Digital Forensik. Pertanyaan ini memicu seberapa antusiasme peserta, sehingga terhibur saat bermain.
- *Novelty* (kebaruan): Tingkat kreativitas dan Inovasi yang dapat menarik minat peserta CTF *Jeopardy-Style* dibidang digital forensik, untuk mengukur sejauh mana peserta menilai permainan ini unik dan berbeda.

Terdapat format kusioner yang telah disediakan UEQ untuk melakukan survey pengalaman user pada penelitian ini, Gambar 3 terdapat 26 item format kusioner.

	1	2	3	4	5	6	7		
menyusahkan	○	○	○	○	○	○	○	menyenangkan	1
tak dapat dipahami	○	○	○	○	○	○	○	dapat dipahami	2
kreatif	○	○	○	○	○	○	○	monoton	3
mudah dipelajari	○	○	○	○	○	○	○	sulit dipelajari	4
bermanfaat	○	○	○	○	○	○	○	kurang bermanfaat	5
membosankan	○	○	○	○	○	○	○	mengasyikkan	6
tidak menarik	○	○	○	○	○	○	○	menarik	7
tak dapat diprediksi	○	○	○	○	○	○	○	dapat diprediksi	8
cepat	○	○	○	○	○	○	○	lambat	9
berdaya cipta	○	○	○	○	○	○	○	konvensional	10
menghalangi	○	○	○	○	○	○	○	mendukung	11
baik	○	○	○	○	○	○	○	buruk	12
rumit	○	○	○	○	○	○	○	sederhana	13
tidak disukai	○	○	○	○	○	○	○	menggembirakan	14
lazim	○	○	○	○	○	○	○	terdepan	15
tidak nyaman	○	○	○	○	○	○	○	nyaman	16
aman	○	○	○	○	○	○	○	tidak aman	17
memotivasi	○	○	○	○	○	○	○	tidak memotivasi	18
memenuhi ekspektasi	○	○	○	○	○	○	○	tidak memenuhi ekspektasi	19
tidak efisien	○	○	○	○	○	○	○	efisien	20
jelas	○	○	○	○	○	○	○	membingungkan	21
tidak praktis	○	○	○	○	○	○	○	praktis	22
terorganisasi	○	○	○	○	○	○	○	berantakan	23
atraktif	○	○	○	○	○	○	○	tidak atraktif	24
ramah pengguna	○	○	○	○	○	○	○	tidak ramah pengguna	25
konservatif	○	○	○	○	○	○	○	inovatif	26

Gambar 3: Item Pertanyaan

Pertanyaan kusioner yang telah disesuaikan dengan penelitian yang akan diuji:

- *Attractiviness* (daya tarik)
  a. Sejauh mana Anda menilai CTF Jeopardy-Style menyediakan tantangan yang menarik dan membuat proses belajar khususnya digital forensik menyenangkan?
  b. Sejauh mana CTF Jeopardy-Style memberikan masalah dan tantangan yang unik dalam belajar digital forensik?
  c. Bagaimana perasaan Anda, saat harus

mengandalkan informasi atau keahlian rekan tim dalam menyelesaikan tantangan CTF Jeopardy-Style?
d. Pada skala berikut, seberapa nyaman Anda dengan pembagian tanggung jawab dalam tim Anda saat berpartisipasi dalam CTF Jeopardy-Style?
e. Bagaimana Anda menilai materi yang digunakan dalam CTF Jeopardy-Style khususnya materi terkait digital forensik?
f. Bagaimana instruksi dan petunjuk dalam CTF Jeopardy-Style digital forensik?

- *Efficiency* (efisiensi):
  a. Bagaimana Anda menilai kecepatan belajar digital forensik yang dihasilkan melalui penggunaan CTF Jeopardy-Style?
  b. Dalam menyelesaikan tantangan CTF Jepardy-Style digital forensik, seberapa efisien Anda menilai alur dari instruksi ke penyelesaian tantangan?
  c. Bagaimana menurut anda pembelajaran CTF Jepardy-Style digital forensik dalam penerapannya di situasi nyata atau studi lanjutan?
  d. Seberapa baik struktur dan urutan materi dalam CTF Jeopardy-Style memudahkan proses pembelajaran Anda dalam digital forensik?
- *Perspicuity* (kejelasan):
  a. Seberapa mudah Anda memahami konsep dan aturan dalam CTF Jeopardy-Style ketika pertama kali diperkenalkan kepada Anda?
  b. Seberapa mudah bagi anda dalam menyelesaikan CTF Jeopardy-Style digital forensik secara mandiri mengikuti instruksi yang telah diberikan?
  c. Saat pertama kali menghadapi tantangan dalam CTF Jeopardy-Style digital forensik, bagaimana Anda menilai proses untuk memahami apa yang diminta?
  d. Seberapa jelas instruksi dan pedoman yang diberikan sebelum dan selama kegiatan CTF Jeopardy-Style digital forensik?
- *Dependability* (ketepatan):
  a. Saat berpartisipasi dalam CTF Jeopardy-Style, seberapa dapat diprediksikah tindakan rekan tim Anda dalam merespon tantangan yang diberikan?
  b. Apakah CTF Jeopardy-Style dapat membantu Anda merasa termotivasi untuk mengejar pengetahuan lebih dalam terkait digital forensik?
  c. Dalam situasi di mana anggota tim Anda tidak dapat menyelesaikan bagian mereka dari tantangan, seberapa aman Anda merasa atas kemampuan tim Anda untuk mengatasi masalah dan tetap maju?
  d. Bagaimana proses pembelajaran melalui CTF Jeopardy-Style dalam hal meningkatkan pengalaman Anda dibidang digital forensik?
- *Stimulation* (stimulasi):
  a. Seberapa bermanfaat CTF Jeopardy-Style dalam meningkatkan pemahaman Anda tentang konsep-konsep digital forensik?
  b. Apakah CTF Jeopardy-Style menarik minat Anda untuk belajar lebih dalam tentang digital forensik?
  c. Berdasarkan pengalaman Anda, seberapa mengasyikkan aktivitas CTF Jeopardy-Style dalam mempelajari digital forensik?
  d. Sejauh mana CTF Jeopardy-Style memotivasi Anda untuk lebih dalam belajar tentang digital forensik?
- *Novelty* (kebaruan):
  a. Bagaimana Anda menilai tingkat kreativitas dalam desain dan konsep CTF Jeopardy-Style terutama dalam bidang digital forensik?
  b. Dalam menyelesaikan soal-soal CTF Jepardy-Style digital forensik, apakah anda merasa bahwa proses untuk menemukan solusi lebih cenderung bersifat eksploratif dan inovatif atau mengikuti metode yang sudah umum?
  c. Seberapa sering CTF Jeopardy-Style ini menyajikan ide-ide baru dan cara-cara inovatif dalam belajar digital forensik yang belum Anda temui sebelumnya?
  d. Bagaimana pendapat Anda tentang konsep soal dalam CTF Jeopardy-Style? Apakah konsep tersebut memberikan cara baru dalam memecahkan masalah digital forensik?

3.4 Uji Reabilitas Data

Uji reabilitas data pada penelitian ini menggunakan *Alpha Cronbach*. Uji reabilitas data dilakukan untuk menguji apakah data yang digunakan dalam analisis lanjutan data realibel atau konsisten. Tidak ada aturan yang secara umum mengatur seberapa besar nilai koefisien tersebut seharusnya. Terdapat beberapa peneliti yang beranggapan bahwa *Alpha Cronbach* > 0,60 atau 0.70 adalah nilai yang dianggap cukup konsisten, namun dalam menentukan nilai *Alpha Cronbach* harus diinterpretasikan dengan sangat hati - hati, karena dapat menyebabkan masalah terhadap skala yang diuji nantinya. Hal ini harus disertakan perhitungan interval kepercayaan 5% [21]. Semakin kecil nilai interval kepercayaan, maka semakin tinggi nilai perkiraan skala terebut dapat dipercaya dan begitu juga sebaliknya.

3.5 *Data Analysis Tools (DAT)*

Data yang diperoleh menggunakan UEQ dapat diolah menggunakan *Data Analysis Tools (DAT)*. Hasil data yang diperoleh dari responden, kemudian dimasukkan ke DAT. Penilaian dari responden terhadap 26 item pertanyaan dengan poin skala 1 sampai 7. Pasangan item pertanyaan yang bertolak belakang secara makna mempresentasikan pengalaman dari user terhadap penelitian ini. Setiap skala pada item yang

diperoleh dipresentasikan dari skala –3 mewakili jawaban paling negatif, 0 merupakan jawaban netral, dan +3 mewakili jawaban paling positif. Beberapa item pertanyaan dimulai dengan istilah negatif dan lainnya istilah positif. Namun terdapat juga beberapa item pertanyaan yang dimulai dengan sebaliknya. Hal ini terjadi dalam urutan acak.

3.6 Uji Regresi

Penelitian ini menggunakan uji regresi berganda *(multiple regression)* dengan tujuan untuk memprediksi seberapa besar pengaruh variabel X terhadap variabel Y[22]. Kriteria pengujian analisis regresi digunakan untuk membandingkan nilai signifikansi dalam membuktikan hipotesis dari jawaban sementara yang akan dibuktikan kebenarannya[22]. Berikut hipotesis yang diajukan:

- H_0 : *Capture The Flag Jeopardy-Style* tidak berpengaruh positif dan signifikan terhadap memperkenalkan pendidikan digital forensik berdasarkan skala *attractiviness, perspicuity, efficiency, dependability, stimulation, novelty*.
- H_a : *Capture The Flag Jeopardy-Style* berpengaruh positif dan signifikan terhadap memperkenalkan pendidikan digital forensik berdasarkan skala *attractiviness, perspicuity, efficiency, dependability, stimulation, novelty*.

Beberapa konsep dasar analisis regresi berganda:

- Uji T : Menentukan ada tidaknya pengaruh parsial (sendiri) yang diberikan oleh variabel X terhadap variabel Y[22]. Dimana derajat signifikansi yang digunakan adalah 0,05. Hipotesis alternatif diterima jika nilai signifikan kurang dari derajat kepercayaan atau t hitung lebih dari t tabel. Hipotesis ini mengatakan bahwa variabel Y secara parsial dipengaruhi oleh variabel X[22].
- Uji F : Menentukan ada atau tidaknya pengaruh secara simultan (bersama-sama) yang diberikan oleh variabel X terhadap variabel Y[22]. Dimana derajat signifikansi yang digunakan adalah 0,05. Hipotesis alternatif diterima jika nilai signifikan kurang dari derajat kepercayaan atau f hitung lebih dari f tabel[20]. Hipotesis ini mengatakan bahwa variabel X secara simultan mempengaruhi variabel Y.
- Koefisien Diterminasi : Menentukan persen pengaruh oleh variabel X terhadap variabel Y[22].

4. Hasil dan Pembahasan

4.1 Pembuatan Soal Bidang Digital Forensik

Pembuatan soal CTF digital forensik pada platform HarisCTF dibuat dengan tujuan untuk memberikan pengalaman dan meningkatkan pemahaman terkait digital forensik bagi pemula. Soal - soal yang telah dibuat disesuaikan dengan tingkat kesulitan soal berdasarkan poin yang tertera.

Gambar 4: Platform HarisCTF

Gambar 5: Tingkatan Poin

Beberapa kategori digital forensik pada soal yang telah dibuat:

4.1.1 Steganografi

Steganografi adalah teknik menyembunyikan pesan tersembunyi di dalam sebuah media, sehingga keberadaan pesan tersebut tidak dapat dilihat secara langsung. Dengan metode steganografi, para pelaku kejahatan siber juga memanfaatkannya untuk menyembunyikan kejahatan mereka di tempat yang tidak terlihat mencurigakan[23][24]. Terdapat banyak tools steganografi yang dapat digunakan seperti *strings, binwalk, exiftool, steghide, zsteg,* dan lainnya[25]. Beberapa soal yang dibuat pada platform HarisCTF dengan menggunakan pengimplementasian steganografi sebagai berikut.

- WTB

Gambar 6: Soal WTB

- MetaFile

Gambar 7: Soal Meta File

- Jembatan Barelang

Gambar 8: Soal Jembatan Barelang

- Sembunyikan Saya

Gambar 9: Soal Sembunyikan Saya

- Bukan PDF Biasa

Gambar 10: Soal Bukan PDF Biasa

4.1.2 Spektogram

Spektogram audio adalah visualisasi spektrum frekuensi sinyal audio, yang memungkinkan analis forensik memvisualisasikan karakteristik frekuensi rekaman audio. Dalam konteks analisis digital forensik, spektogram audio menjadi alat yang penting untuk mengekstraksi informasi seperti deskripsi file, waktu modifikasi, dan hash yang dapat digunakan sebagai bukti digital dalam investigasi forensik. Keunggulan spektogram termasuk kemampuannya untuk memvisualisasikan perubahan frekuensi dari waktu ke waktu, mengidentifikasi gangguan atau manipulasi dalam rekaman audio, dan mendeteksi pola yang mencurigakan atau tidak biasa[26]. Sebagai contoh pengimplementasian pada soal yang dibuat pada gambar 11.

Gambar 11: Soal Nyanyian

4.1.3 Image File Format

Penyembunyian pesan rahasia tidak hanya melibatkan metode steganografi yang mencakup penyisipan pesan dalam metadata file, tetapi juga dapat dilakukan dengan cara menyembunyikan pesan dalam struktur atau konten file itu sendiri. Metode ini seringkali melibatkan manipulasi data biner pada berbagai jenis file, seperti gambar, audio, video, atau dokumen teks[27]. Contoh-contoh teknik yang digunakan termasuk menyisipkan pesan dalam bit yang kurang signifikan dalam gambar. Pendekatan semacam ini memungkinkan komunikasi rahasia tanpa menimbulkan kecurigaan, karena pesan tersebut tersembunyi dalam format *file* yang tampaknya biasa. *File* gambar biasa berisi banyak informasi. Struktur umum file gambar terutama mencakup tiga bagian yaitu *file header*, *file body*, dan *file end*[28]. Contoh soalnya pada gambar 12.

Gambar 12: Soal Sisipan

4.1.4 Memory Forensic

Permasalahan keamanan siber meningkat karena ancaman malware tanpa file yang sulit dideteksi. Malware semacam ini, sulit terdeteksi karena tidak meninggalkan jejak dalam sistem file, sehingga menghambat upaya identifikasi. Data penting yang diperlukan untuk melacak keberadaan dan aktivitas

malware seringkali tersimpan dalam memori volatil, seperti RAM, yang sulit diakses menggunakan metode tradisional[29][30]. Salah satu alat yang banyak digunakan untuk melakukan analisis forensik memori adalah *Volatility*, yang merupakan *tool open source* yang populer di kalangan peneliti dan organisasi berukuran menengah. Upaya ini menjadi langkah penting dalam memahami cara terbaik untuk melindungi sistem dari ancaman malware yang semakin canggih[31]. Soal yang dibuat pada gambar 13 dan 14.

- *Memory Dump Part 1*

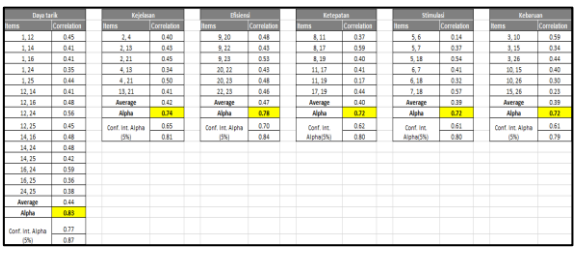
Gambar 13: Soal Memory Dump 1

- *Memory Dump Part 2*

Gambar 14: Soal Memory Dump 2

4.2 Uji Reabilitas Data

Pengujian ini menggunakan *tool* yang sudah disediakan oleh UEQ. Dilihat dari gambar berikut bahwa nilai *Alpha Cronbach* memenuhi dan jawaban dari responden dianggap dapat dipercaya.



Gambar 15: Perhitungan Alpha Cronbach

4.3 Analisis Data

Hasil jawaban dari responden yang telah terkumpul, dimasukkan dan dilakukan pengujian serta analisis berdasarkan UEQ *Data Analysis Tool*.

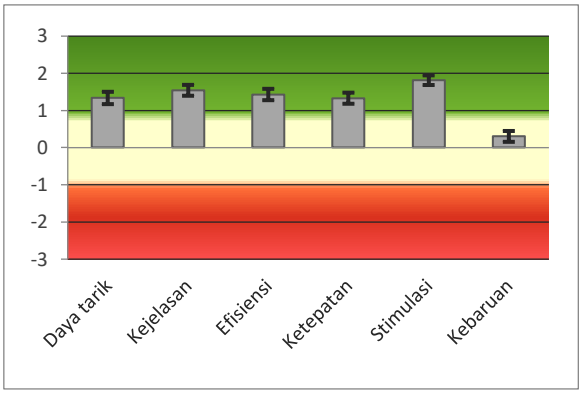
	Items																								
2																									
3	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
4	6	6	2	2	2	6	6	6	2	4	6	2	6	6	6	6	2	2	3	6	1	6	2	1	1	5
5	6	6	1	1	2	6	6	6	2	4	6	2	6	6	4	6	3	2	2	6	3	6	2	2	2	4
6	5	4	4	4	3	5	4	4	4	4	6	4	3	5	4	4	4	3	3	5	4	4	4	3	3	5
7	7	7	1	1	1	7	7	6	2	3	6	2	7	7	5	7	1	1	1	7	1	7	1	1	1	5
8	5	6	2	2	1	5	6	5	2	4	6	3	6	5	4	5	4	3	1	5	3	6	1	3	1	5
9	7	6	2	3	1	7	7	7	2	3	7	2	6	7	5	7	1	1	3	6	2	6	2	1	1	5
10	7	7	1	1	1	7	7	7	1	3	7	1	7	7	5	7	1	1	1	7	1	7	1	1	1	6
11	6	5	2	3	2	5	6	6	3	3	6	3	5	5	5	6	3	2	3	6	3	5	2	3	2	5
12	7	6	1	2	1	7	7	6	1	2	7	1	6	7	5	7	1	1	1	6	1	7	1	1	1	4
13	7	7	1	1	1	7	7	7	1	1	7	1	7	7	5	7	1	1	1	7	1	7	1	1	1	5
14	7	7	1	1	1	7	7	7	1	3	7	1	7	7	6	7	1	1	1	7	1	7	1	1	1	4
15	7	7	1	2	1	7	7	7	2	4	7	2	6	7	5	7	2	1	1	7	2	7	1	1	1	5
16	6	6	1	1	1	6	7	6	1	3	7	2	7	7	5	7	1	1	1	7	1	7	1	1	1	6
17	5	6	2	2	1	6	5	6	2	3	7	2	5	7	5	7	2	2	2	6	1	7	3	2	3	4
18	6	7	2	3	1	5	6	5	4	4	7	2	4	5	4	5	3	3	3	4	3	4	3	2	2	5
19	7	6	4	3	1	4	6	6	1	3	6	3	4	6	4	6	2	3	4	7	4	7	4	3	4	4
20	5	5	2	3	2	5	7	5	3	4	5	2	6	5	5	6	4	3	2	5	2	4	2	1	3	5
21	5	5	1	4	3	6	7	5	4	3	5	1	6	5	4	5	3	4	3	4	3	5	3	2	3	5
22	6	5	1	1	1	6	6	6	3	3	6	2	6	5	5	6	3	2	2	6	2	6	3	2	1	4
23	7	6	2	2	1	6	5	6	3	3	7	1	7	6	4	7	1	4	2	6	3	7	1	1	1	4
24	7	7	3	2	1	5	6	7	1	3	6	2	7	7	5	7	3	1	2	7	1	7	1	2	1	5
25	7	7	1	1	1	7	7	7	1	2	7	1	7	7	5	7	1	1	1	7	1	7	1	1	1	5
26	6	6	2	1	1	6	6	5	2	4	5	2	6	5	5	6	3	3	2	6	1	6	1	2	2	5
27	5	4	4	4	2	6	6	4	4	4	7	4	4	4	4	5	4	3	3	4	4	5	4	4	3	6
28	7	7	1	2	1	7	7	7	1	3	7	1	7	7	4	7	2	1	1	7	1	7	2	1	1	4
29	7	7	1	1	1	7	7	7	1	1	7	1	7	7	5	7	1	1	1	7	1	7	1	1	1	5
30	6	6	1	2	1	6	6	6	2	3	6	2	5	7	4	6	2	1	3	6	2	7	1	2	2	6
31	7	7	1	1	1	7	7	7	1	2	7	1	6	7	5	7	1	1	1	7	1	7	1	1	1	4
32	6	6	2	3	1	6	6	6	2	4	6	2	6	6	5	6	2	2	2	6	2	6	2	2	2	6
33	7	7	1	1	1	7	7	7	1	3	7	1	7	7	5	7	1	1	1	7	1	7	1	1	1	4
34	5	4	2	2	3	4	4	4	4	4	5	2	4	4	4	4	4	4	4	4	4	4	4	3	3	4
35	6	6	5	2	1	7	7	5	2	4	5	3	7	7	4	7	3	1	3	4	1	5	1	2	2	5
36	5	6	3	3	3	6	5	6	2	3	6	4	6	6	5	6	3	2	3	5	3	5	2	2	3	5
37	4	4	4	4	3	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	5
38	4	4	4	4	3	4	4	4	4	4	4	4	5	4	5	4	4	4	3	4	4	4	3	4	4	4
39	7	6	2	2	2	5	7	5	2	3	6	3	6	6	5	6	1	1	2	6	3	5	1	1	1	5
40	4	4	4	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	3	4	4	3	3	5
41	5	5	3	3	3	5	5	5	3	3	5	3	5	5	4	5	3	3	3	5	3	5	3	3	3	5
42	6	4	2	2	3	6	6	5	2	3	4	3	4	4	5	6	4	4	2	5	2	4	3	1	2	5
43	7	7	1	1	1	6	7	6	4	3	7	2	7	7	4	7	1	1	1	7	1	7	2	2	1	4
44	6	6	5	3	1	6	6	4	4	5	6	4	6	5	4	5	4	1	4	6	3	5	2	4	2	4
45	7	6	4	2	2	6	6	6	4	4	7	4	5	6	5	4	4	4	3	6	2	5	3	4	2	4
46	6	6	5	2	1	6	6	6	4	4	6	3	6	5	5	4	4	4	5	6	3	5	2	4	2	4
47	6	6	4	2	2	5	6	5	4	4	6	3	6	5	5	4	4	4	4	6	2	5	3	4	4	4
48	7	7	5	2	1	6	6	5	4	4	6	4	4	6	5	4	5	4	4	6	2	5	2	3	3	3
49	5	5	4	2	2	5	6	5	4	4	6	2	4	7	5	3	4	4	4	5	1	5	2	3	1	3
50	6	6	5	3	1	6	5	6	4	4	6	2	5	6	5	3	4	4	2	6	2	6	2	4	1	3
51	6	6	4	2	2	5	5	4	3	4	6	2	5	5	3	4	4	3	3	5	3	5	3	3	2	4
52	7	6	5	3	1	6	5	6	3	5	6	2	5	6	5	3	4	3	2	6	2	5	4	2	3	3
53	5	6	4	3	1	5	5	5	3	5	7	2	5	5	5	3	4	3	2	7	1	5	5	3	1	3
54	6	6	5	3	1	6	5	4	3	5	7	2	5	6	4	3	5	3	2	5	1	6	3	4	1	3
55	5	5	4	3	1	5	5	4	3	5	6	3	5	5	5	2	4	4	3	4	1	7	3	2	3	4
56	5	6	5	4	1	6	5	4	5	4	7	3	5	5	3	2	5	3	3	4	1	6	3	4	2	3
57	5	5	4	4	1	5	5	6	5	5	7	2	5	6	3	3	4	4	2	4	2	5	3	3	2	5
58	6	7	5	3	1	6	5	6	5	4	6	3	7	7	5	3	5	3	3	5	2	5	4	3	4	4
59	5	5	5	1	2	6	4	6	5	5	5	2	6	5	5	3	4	3	3	4	2	5	4	4	4	4
60	6	7	4	3	2	5	4	6	5	5	5	3	5	6	5	2	5	3	3	5	3	6	2	3	3	3
61	5	5	4	3	2	7	4	6	5	5	5	3	5	4	5	2	4	3	3	6	2	6	3	4	3	3
62	6	7	5	3	2	5	4	6	3	5	5	2	4	5	5	2	5	3	3	5	3	6	2	3	3	5
63	7	5	4	3	2	7	4	6	5	4	7	3	4	4	4	2	4	4	2	6	2	5	3	3	2	5
64	6	4	5	3	3	6	4	6	4	5	6	2	4	4	4	2	4	4	2	7	3	5	2	2	2	5
65	5	4	5	3	3	7	5	6	3	5	7	2	5	4	4	2	4	4	2	5	4	5	3	2	2	5
66	6	6	5	3	3	7	6	5	5	4	6	2	4	4	4	1	5	4	2	7	3	5	2	4	2	5
67	6	5	4	2	3	7	6	5	3	4	5	2	6	5	5	1	5	4	2	5	2	6	3	2	3	4
68	7	4	4	2	3	7	5	5	3	3	5	2	5	5	5	1	5	4	2	5	3	6	2	3	2	4
69	5	6	4	2	1	6	5	5	3	3	5	3	6	6	5	3	5	4	2	5	2	6	3	2	3	4
70	4	7	4	2	1	5	5	5	4	3	6	3	5	6	5	4	5	3	3	4	3	6	2	2	3	4
71	4	5	4	4	1	6	5	5	4	4	6	3	5	5	4	2	5	3	3	5	4	7	3	3	2	4
72	6	5	4	4	1	5	6	5	4	4	6	3	6	6	4	1	5	3	2	6	3	6	2	4	2	3
73	7	5	5	5	2	6	6	4	4	4	6	3	6	5	3	4	4	3	3	5	2	5	3	2	2	4
74	3	6	5	5	2	6	6	4	4	4	6	4	6	4	3	3	5	3	2	4	4	6	2	3	2	3
75	4	6	5	3	2	6	6	4	4	5	6	4	6	6	3	2	4	3	3	5	3	5	3	3	2	4
76	3	7	5	3	2	6	6	4	3	4	6	3	6	6	3	1	4	3	2	6	2	6	2	4	3	3
77	5	6	3	4	2	6	6	4	3	4	6	3	6	7	3	2	5	3	3	5	4	6	3	2	3	4
78	6	5	3	2	1	6	6	4	3	4	6	3	6	5	3	2	4	3	3	3	3	5	3	3	2	3
79	7	5	4	2	1	6	6	4	3	5	5	2	6	5	3	2	5	3	3	4	2	6	2	3	3	4
80	4	7	4	2	2	5	6	5	4	5	5	3	5	5	4	1	4	3	2	5	3	7	2	3	2	4
81	5	6	4	2	2	6	6	4	3	5	5	3	5	5	4	1	5	3	2	4	4	7	3	2	3	3
82	6	6	3	3	2	6	6	5	4	4	5	2	5	5	4	3	4	4	2	4	4	7	3	3	2	3
83	5	5	4	3	2	6	6	4	4	5	6	3	5	5	3	3	3	3	2	6	5	6	2	2	3	4
84	5	5	5	3	2	6	6	6	3	5	5	3	5	6	4	1	4	3	2	5	5	5	3	3	1	3
85	6	4	5	3	2	6	6	5	4	4	5	3	6	6	3	2	5	3	2	6	4	6	3	3	1	4
86	7	5	3	2	2	6	5	5	3	5	5	3	6	6	4	2	4	3	2	5	4	7	3	2	2	4
87	6	5	3	3	2	7	5	4	4	4	6	3	6	6	4	2	5	3	2	6	3	6	2	2	3	4
88	5	6	3	5	2	7	5	5	4	4	7	4	6	6	3	3	3	3	3	6	5	6	2	2	2	4
89	5	5	3	4	2	7	5	5	3	6	6	3	6	6	4	2	4	3	3	5	3	5	2	4	3	5
90	6	4	3	5	2	7	5	6	3	4	6	4	6	6	3	2	5	3	3	5	2	6	2	4	2	4
91	6	5	4	2	2	7	5	5	3	5	7	3	6	6	4	3	5	3	3	5	2	7	3	2	1	4
92	7	4	4	2	2	5	5	5	4	4	7	4	5	6	3	2	3	4	3	5	3	6	3	4	2	3
93	7	6	4	2	1	5	5	5	4	4	5	3	5	5	4	3	3	3	3	5	2	7	3	2	3	4
94	5	6	4	2	1	5	5	5	4	4	6	4	5	5	3	2	3	3	3	6	3	6	2	4	2	4
95	4	6	3	2	1	6	5	4	4	4	6	3	5	6	4	3	3	2	3	5	2	5	2	2	3	4
96	5	5	3	3	1	5	5	6	4	6	6	3	5	6	3	2	3	2	3	6	3	6	2	2	2	4
97	6	7	4	3	1	6	6	6	4	4	6	3	5	5	3	3	3	1	3	5	2	7	2	4	1	4
98	7	5	4	4	1	5	5	6	4	6	7	3	6	5	3	2	4	2	4	6	3	7	3	2	1	4
99	5	6	4	3	1	6	5	6	4	6	6	3	6	6	3	3	4	2	5	5	3	6	3	2	2	4
100	4	5	3	2	1	5	5	6	4	6	7	3	6	5	4	2	4	1	4	6	2	7	2	2	3	4
101	5	6	3	3	1	6	6	5	4	5	7	3	6	5	4	2	4	1	4	5	2	6	3	2	2	4
102	6	6	4	4	1	6	6	4	4	4	7	4	6	5	4	2	4	1	4	5	2	6	2	3	3	4
103	6	5	4	3	1	6	6	4	4	6	7	3	6	5	4	2	4	2	5	5	3	6	3	4	2	4

Gambar 16: Data Responden

Hasil rata-rata skala UEQ yang diperolah beserta grafiknya dapat dilihat pada tabel 1 dan gambar 17.

Tabel 1: Rata-rata skala UEQ dalam pengujia

UEQ Scales (Mean and Variance)		
Daya tarik	1.337	0.71
Kejelasan	1.543	0.56
Efisiensi	1.430	0.61
Ketepatan	1.330	0.58
Stimulasi	1.815	0.44
Kebaruan	0.303	0.55

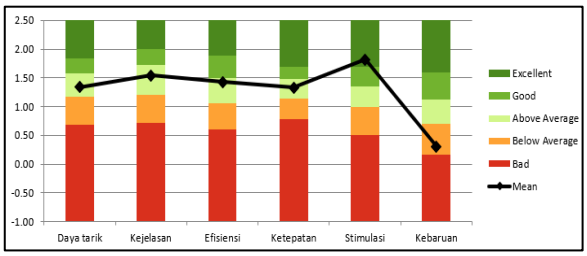


Gambar 17: Grafik rata-rata skala UEQ dalam pengujian

Hasil perbandingan uji Benchmark UEQ dapat dilihat pada tabel 2 dan gambar 18.

Tabel 2: Uji Benchmark

Scale	***Mean***	***Comparisson to benchmark***	***Interpretation***
Daya tarik	1.34	*Above average*	25% hasil lebih baik, 50% hasil lebih buruk
Kejelasan	1.54	*Above Average*	25% hasil lebih baik, 50% hasil lebih buruk
Efisiensi	1.43	*Above Average*	25% hasil lebih baik, 50% hasil lebih buruk
Ketepatan	1.33	*Above Average*	25% hasil lebih baik, 50% hasil lebih buruk
Stimulasi	1.82	*Excellent*	Dalam rentang 10% hasil terbaik
Kebaruan	0.30	*Below Average*	50% hasil lebih baik, 25% hasil lebih buruk



Gambar 18: Grafik uji Benchmark

Terlihat pada gambar di atas, bahwa nilai rata-rata dari 6 skala UEQ berada pada batas warna hijau muda. Hal ini diartikan keseluruhan skala pengukuran berada pada level yang diatas rata-rata. Skala daya tarik *(attractiveness)* mendapatkan nilai 1.34 yang artinya *Above average*, kejelasan *(perspicuity)* mendapatkan nilai 1.54 yang artinya *Above average*, efiesiensi *(efficiency)* mendapatkan nilai 1,43 yang artinya *Above average*, ketepatan *(dependability)* mendapatkan nilai 1,33 yang artinya *Above average* , stimulasi *(stimulation)* mendapatkan nilai 1,82 yang artinya *excellent* dan kebaruan mendapatkan nilai 1,09 yang artinya *bellow average*.

Dapat diketahui bahwa pembelajaran pada platform HarisCTF memberikan motivasiyang tinggi bagi penggunanya dalam bermain CTF dibidang digital forensik, dinilai dari skala stimulasi yang berada pada nilai paling tinggi diantara skala lainnya. Untuk 4 skala lainnya yaitu daya tarik, kejelasan, efisiensi, dan ketepatan dinilai diatas rata-rata yang artinya cukup dalam memberikan kesan, intruksi atau alur pada soal, dan interaksi peserta mengandalkan tim saat bermain CTF di platform HarisCTF. Pada skala kebaruan terletak di warna oren yang artinya dibawah rata - rata. Hal ini dapat menjadi evaluasi dalam meningkatkan kreativitas dan Inovasi yang dapat menarik minat peserta CTF Jeopardy-Style dibidang digital forensik pada platform HarisCTF.

4.4 Uji Regresi

4.4.1 Uji T

$$t\ tabel = t\left(\frac{\alpha}{2}; n-k-1\right) = t(0{,}025; 93)$$
$$= 1{,}986$$

Dengan penjelasan:
n = sampel
k = jumlah variable X

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	-.017	.032		-.546	.586
	X1	.164	.008	.227	20.335	<.001
	X2	.167	.007	.203	22.508	<.001
	X3	.180	.008	.228	22.886	<.001
	X4	.163	.006	.179	28.374	<.001
	X5	.160	.009	.169	17.237	<.001
	X6	.166	.008	.185	22.151	<.001

Gambar 19: SPSS uji t

Dari hasil pengolahan data, diperoleh hasil uji nilai t hitung variabel X1 (20,335), X2 (22,508), X3 (22,886), X4(28,374), X5(17,237), dan X6 (22,151) dinilai lebih dari nilai t tabel (1,986), yang artinya membuktikan bahwa variabel Y secara parsial dipengaruhi oleh variabel X.

4.4.2 Uji F

$$F\ tabel = F(k; n-k) = F(6;;94) = 2{,}197$$

Dengan penjelasan:
n = sampel
k = jumlah variable X

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	37.181	6	6.197	6037.908	<.001[b]
	Residual	.095	93	.001		
	Total	37.276	99			

Gambar 20: SPSS uji f

Dari hasil pengolahan data, diperoleh hasil uji nilai f hitung variabel X1 6037.908 > 2,197, yang artinya membuktikan bahwa variabel X secara simultan mempengaruhi variabel Y.

4.4.3 Koefisien Diterminasi

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.999[a]	.997	.997	.03204

Gambar 20: Koefisien diterminasi

Dari hasil uji diatas bahwa nilai R square sebesar 0,997. Hal ini membuktikan bahwa pengaruh variabel X1, X2, X3, X4, X5, dan X6 terhadap variabel Y benilai 99,7 %.

5. Kesimpulan

Pendidikan keamanan siber menjadi hal yang krusial di era digitalisasi saat ini. Konsep gamifikasi, terutama melalui *Capture The Flag (CTF*), telah terbukti efektif dalam meningkatkan pemahaman dan keterampilan dalam keamanan siber. Platform CTF *Jeopardy-Style*, khususnya dalam bidang digital forensik, memberikan landasan yang penting dalam pengembangan keahlian yang diperlukan untuk melawan kejahatan digital. Keterkaitan antara CTF dan digital forensik memberikan dasar yang kuat bagi peserta untuk memahami teknik digital forensik dengan lebih baik. Berdasarkan hasil analisis yang telah dilakukan pada pengujian diatas, dapat diberi kesimpulan dari 26 item pertanyaan UEQ dikelompokkan menjadi enam skala, penilaian dari keenam skala, untuk skala stimulasi dinilai baik sekali, skala daya tarik, kejelasan, efisiensi, dan ketepatan dinilai diatas rata-rata, dan skala kebaruan dinilai dibawah rata-rata. Artinya platform HarisCTF memberikan kesan baik dan bermanfaat bagi pengguna untuk mempelajari digital forensin, namun perlu evaluasi untuk meningkatkan skala kebaruan. Pada uji regresi hipotesis membuktikan bahwa *Capture The Flag Jeopardy-Style* tidak berpengaruh positif dan signifikan terhadap memperkenalkan pendidikan digital forensik berdasarkan skala *attractiviness, perspicuity, efficiency, dependability, stimulation, novelty.*

6. Daftar Pustaka

[1] S. Karagiannis and E. Magkos, “Adapting CTF Challenges into Virtual Cybersecurity Learning Environments,” Nov. 2020.

[2] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, “Cybersecurity knowledge and skills taught in capture the flag challenges,” Comput Secur, vol. 102, Mar. 2021, doi: 10.1016/j.cose.2020.102154.

[3] L. Ken Chen, M. Hanis Jenalis, and J. Juremi, “Towards Inclusive Cybersecurity Learning: A Novice-Friendly Capture-the-Flag Onboarding Platform,” 2023.

[4] J. Holmi, “Advantages and challenges of using capture-the-flag games in cyber security education,” 2020. doi: 10.1108/ICS-04-2019-0050.

[5] K. H. Tan and E. L. Ouh, “Lessons learnt conducting Capture the Flag CyberSecurity Competition during COVID-19,” 2021. doi: 10.1109/FIE49875.2021.9637404.

[6] S. V. Cole, “Impact of Capture The Flag (CTF)-style vs. Traditional Exercises in an Introductory Computer Security Class,” ACM Conference on Innovation and Technology in Computer Science Education, ITiCSE, Jul. 2022, pp. 470–476. doi: 10.1145/3502718.3524806.

[7] J. T. T, J. G. A, and Nelmiawati, “Analysis of Cyber Security Knowledge and Skills for Capture the Flag Competition,” Apr. 2022.

[8] R. G. Chicone and S. Ferebee, “A Comparison Study of Two Cybersecurity Learning Systems: Facebook’s Open Source Capture The Flag And Ctfd,” Issues in Information Systems, vol. 21, no. 1, pp. 202–212, 2020, doi:

10.48009/1_iis_2020_202-212.

[9] K. N. Isnaini and W. Widodo, “Digital Forensic Tools And Techniques For Handling Digital Evidence,” Jurnal Resistor, vol. 6, 2023, doi: https://doi.org/10.31598.

[10] S. Naqvi, P. Sommer, and M. Josephs, A Research-Led Practice-Driven Digital Forensic Curriculum to Train Next Generation of Cyber Firefighters. IEEE Global Engineering Education Conference (EDUCON), 2019. doi: 10.1109/EDUCON.2019.8725129.

[11] K. Michaylov, “Exploring the Use of Steganography and Steganalysis in Forensic Investigations for Analysing Digital Evidence,” Netherlands, Jul. 2023.

[12] A. H. A. Hanafi, H. Rokman, A. D. Ibrahim, Z.-A. Ibrahim, M. N. A. Zawawi, and F. A. Rahim, “A Scenario CTF-Based Approach in Cybersecurity Education for Secondary School Students,” 2021. doi: 10.52650/ejcsit.v7i1.107.

[13] R. Taufik, R. L. Bau, and A. Setyanto, “Adaptasi Skala User Experience Questionnaire Dalam Pengujian User Experience Sistem Repositori,” Jurnal Teknologi Informasi , vol. XV, 2020.

[14] T. Balon and I. (Abe) Baggili, “Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education,” Educ Inf Technol (Dordr), vol. 28, no. 9, pp. 11759–11791, Sep. 2023, doi: 10.1007/s10639-022-11451-4.

[15] J. Holmi, “Advantages and challenges of using capture-the-flag games in cyber security education,” 2020.

[16] S. Karagiannis, E. Maragkos-Belmpas, and E. Magkos, “An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools.” [Online]. Available: http://www.springer.com/series/6102

[17] K. Khanza Pangestu, T. L. M. Suryanto, and A. Pratama, “User Experience Questionnaire (UEQ) Sebagai Metode Pengukuran Evaluasi Pengalaman Pengguna Virtual Campus Tour Upn,” 442 Journal of Information System, Applied, Management, Accounting and Research, vol. 7, no. 2, pp. 442–451, 2023, doi: 10.52362/jisamar.v7i2.718.

[18] M. Surahman, N. Widiyasono, and R. Gunawan, “Analisis Usability Dan User Experience Aplikasi Konsultasi Kesehetan Online Menggunakan System Usability Scale Dan User Experience Questionnaire,” Jurnal Siliwangi, vol. 7, no. 1, 2021.

[19] G. N. Ayuni and D. Fitrianah, “Penerapan Metode Regresi Linear Untuk Prediksi Penjualan Properti pada PT XYZ,” Jurnal Telematika, vol. 14, no. 2.

[20] M. Fadhil, “Pengaruh Pembiayaan Modal Kerja Terhadap Pendapatan Usaha Mikro, Kecil Dan Menengah Pada Koperasi Syariah Mitra Niaga,” Banda Aceh, 2019.

[21] M. Schrepp, “User Experience Questionnaire Handbook,” 2023.

[22] N. Sudariana and M. M. Yoedani, “Analisis Statistik Regresi Linier Berganda.”

[23] I. Pujianto and D. Darwis, “Uji Ketahanan Citra Digital Terhadap Manipulasi Robustness Pada Steganography,” Jurnal Informatika dan Rekayasa Perangkat Lunak (JATIKA), vol. 2, no. 1, 2021.

[24] M. Jerry Prabowo and R. Wanto, “Implementasi Steganografi Berbasis Mobile Menyembunyikan PesanGambar Dan Suara,” JURNAL MERDEKA INFORMATIKA, vol. 1, no. 1, 2023.

[25] Dr. N. Arora, “Types and Tools of Steganography,” Int J Res Appl Sci Eng Technol, vol. 10, no. 6, pp. 2049–2053, Jun. 2022, doi: 10.22214/ijraset.2022.44279.

[26] Y. Ren, D. Liu, Q. Xiong, J. Fu, and L. Wang, “Spec-ResNet: A General Audio Steganalysis Scheme based on a Deep Residual Network for Spectrograms,” Jan. 2019, [Online]. Available: http://arxiv.org/abs/1901.06838

[27] M. A. Hasan, O. Lawlor, and N. Jahan, “Forensic analysis of binary structures of video files,” in 2021 IEEE 5th International Conference on Cryptography, Security and Privacy, CSP 2021, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 200–204. doi: 10.1109/CSP51677.2021.9357570.

[28] W. Zhenhua, “Design and Research of an Image File Format with Rich Information,” Journal of Electrical and Electronic Engineering, vol. 6, no. 2, doi: 10.11648/j.jeee.20180602.16.

[29] H. Nyholm et al., “The Evolution of Volatile Memory Forensics,” Journal of Cybersecurity and Privacy, vol. 2, no. 3. Multidisciplinary Digital Publishing Institute (MDPI), pp. 556–572, Sep. 01, 2022. doi: 10.3390/jcp2030028.

[30] R. Shree, A. Kant Shukla, R. Prakash Pandey, V. Shukla, and D. Bajpai, “Memory forensic: Acquisition and analysis mechanism for operating systems,” in Materials Today: Proceedings, Elsevier Ltd, 2021, pp. 254–260. doi: 10.1016/j.matpr.2021.05.270.

[31] P. B. Gadgil and S. Nagpure, Analysis of Advanced Volatile Threats Using Memory Forensics. [Online]. Available: https://ssrn.com/abstract=3358798