STRING (Satuan Tulisan Riset dan Inovasi Teknologi) p-ISSN: 2527 - 9661
Vol. 6 No. 2 Desember 2021 e-ISSN: 2549 - 2837

ANALISIS FORENSIK KONTEN DAN TIMESTAMP PADA APLIKASI TIKTOK

Fauzan Natsir
Program Studi Teknik Informatika, Universitas Indraprasta PGRI
fauzan.natsir@gmail.com

Submitted November 29, 2021; Revised December 4, 2021; Accepted December 4, 2021

Abstrak

Aplikasi Tiktok merupakan salah satu aplikasi *platform social media* yang seringkali banyak celah untuk mendapatkan identitas dari pengguna aplikasi tersebut. TikTok telah mengalami pertumbuhan yang luar biasa dengan mencapai 1,5 miliar pengguna pada tahun 2019. Penelitian ini menggunakan metodologi *Open-Source Intelligence* (OSINT) sebagai standar dalam tahap penelitian untuk mengungkap *timestamp* yang diperoleh dari aplikasi TikTok. Metode yang diterapkan menggunakan pendekatan *National Institute of Standard Technology* (NIST). Penelitian ini menggunakan *tools* forensik yaitu, *Browser History Capture/Viewer, Video Cache Viewer, Unfurl,* dan *Urlebird*. Hasil yang didapatkan di antaranya menunjukkan deskripsi lengkap dari semua artefak digital dan timestamp yang diperoleh dari konten TikTok. Selanjutnya, dengan menggunakan hasil analisis yang dibahas dalam penelitian ini diharapkan dapat merekonstruksi konten dan mencari kata kunci dari *timestamp* di aplikasi TikTok ini.
Kata Kunci : Forensik**,** TikTok, Timestamp

Abstract

The Tiktok application is one of the social media platform applications that often finds many loopholes to get the identity of the application's users. TikTok has experienced tremendous growth by reaching 1.5 billion users in 2019. This research uses an Open-Source Intelligence (OSINT) method as a standard in the research phase to reveal the timestamps obtained from the TikTok application. The method used in this research is the National Institute of Standard Technology (NIST). The research uses forensic tools, namely Browser History Capture/Viewer, Video Cache Viewer, Unfurl and Urlebird. The result of this research shows a complete description of all digital artifacts and timestamps obtained from TikTok content. Furthermore, by using the results of the analysis in the research, it is expected that the research can help to reconstruct the content and to search for keywords from the timestamp in the TikTok application.
Keywords : *Forensics, TikTok, Timestamp*

1. PENDAHULUAN

TikTok merupakan aplikasi platform media sosial konten ramah seluler bentuk pendek telah melihat peningkatan popularitas yang besar selama karantina COVID-19 dan itu hanya berarti satu hal. Dengan banyaknya video yang diunggah pada saat kebanyakan orang berada di rumah selama karantina, sekarang ada lebih banyak cara dan mungkin cara yang lebih mudah untuk menemukan alamat rumah, informasi keluarga, tata letak rumah, dan jadwal kerja orang tersebut. Statistik [1] menyebutkan pengguna menghabiskan rata-rata 46 menit sehari di aplikasi TikTok ini. Oleh karena itu, penting untuk disoroti beberapa potensi masalah privasi dan risiko yang diambil saat menggunakan platform TikTok ini secara maksimal. Platform social media TikTok melalui halaman resminya, menyatakan bahwa aplikasi TikTok sudah menembus 1 miliar pengguna pada masa 27 September 2021. Aplikasi ini pertama

kali dirilis pada September 2016 dan platform TikTok ini hanya membutuhkan waktu 5 tahun untuk menggaet 1 miliar pengguna.

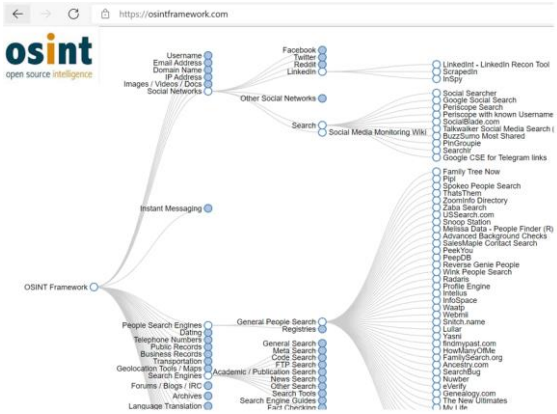
Dilansir dari The Verge [2], popularitas TikTok naik sangat signifikan selama masa pandemi Covid-19 ini yang berawal pada tahun 2020. Pada kuartal pertama tahun tersebut, TikTok menjadi aplikasi paling banyak diunduh, sebanyak 315 juta kali, menurut perusahaan analisis SensorTower. Perusahaan tersebut menaungi TikTok, ByteDance melaporkan pendapatannya pada 2020 mencapai 34,3 miliar dolar AS, melebihi dua kali pendapatan tahun sebelumnya.

Aplikasi TikTok ini semakin populer secara signifikan selama karantina COVID19 dan itu hanya berarti satu hal. Dengan banyaknya video yang diunggah saat kebanyakan orang berada di rumah selama karantina, kini ada lebih banyak, dan mungkin lebih mudah, cara untuk menemukan alamat rumah, informasi keluarga, tata letak apartemen, dan jam kantor [3].

Penelitian terdahulu yang dilakukan [4] dengan judul penelitian "Metode NIST Untuk Analisis Forensik Bukti Digital Pada Perangkat Android" dengan hasil penemuan bukti digital berupa data kontak, log panggilan, dan pesan yang telah dihapus pada smartphone Samsung Galaxy J1 Ace, dapat disimpulkan bahwa recovery dengan tool Wondershare hanya mencapai 30%, sedangkan hasil dari pemulihan dengan forensik oksigen mencapai 73% dari data yang dihapus. Pada penelitian *Facebook Massenger Digital Evidence Analysis Using the NIST Method* yang dilakukan oleh Yudahana et al [5], membahas tentang proses mendapatkan barang bukti pada smartphone android menggunakan software forensik forensik Oxigen pada aplikasi Facebook Massenger. Dengan kesimpulan yaitu hasil yang diperoleh berupa teks percakapan, gambar dan audio. Referensi [6] menjelaskan proses penerapan kasus forensik pada aplikasi pembayaran mobile berbasis Android menggunakan metode penelitian yang mengacu pada pedoman forensik perangkat *mobile* yang dibuat oleh *National Institute of Standards and Technology* (NIST). Dalam proses pengangkatan barang bukti digital untuk *smartphone* yang telah diinstall dengan aplikasi *mobile payment*, diperlukan *rooting* untuk *smartphone* Android, dan ada banyak tools yang dapat digunakan dalam proses pengangkatan barang bukti digital [7].

2. METODE PENELITIAN

Metode penelitian yang digunakan menjelaskan rancangan kegiatan, ruang lingkup atau objek, tempat, teknik pengumpulan data, dan teknik analisis penelitian. Penelitian ini menggunakan pendekatan dengan berbasis *Open Source Intelligence* (OSINT) dengan metodologi multi-faktor (kualitatif dan kuantitatif) untuk mengumpulkan, menganalisis, dan membuat keputusan tentang data yang dapat diakses dari *platform* digital TikTok.[8] Salah satu metode pelacakan OSINT yang digunakan adalah metode *dorking* dengan mencari sebuah kata yang berada di dalam *search engine* untuk mengumpulkan beberapa data seperti *inurl*, *intext* dan lain sebagainya. Berikut beberapa metode yang diterapkan pada pendekatan *framework* OSINT :



Gambar 1. *Framework* OSINT

Tahapan penelitian ini mengacu pada metode *National Institute of Standards and Technology* (NIST) yang terdiri dari beberapa langkah untuk menghasilkan artefak digital dari aplikasi TikTok.[9] Tahapan ini bisa digambarkan sebagai berikut,

Gambar 2. Tahapan *NIST*

Tahapan *National Institute of Standard and Technology* (NIST) mempunyai 4 tahapan yang digunakan untuk melakukan penelitian ini pada proses analisis forensik konten TikTok. Beberapa tahapan pada metode *National Institute of Standards Technology* (NIST), sebagai berikut:

a. Pengumpulan : Tahap ini bertujuan untuk mengidentifikasi, mencatat, dan mengambil data dari sumber data yang relevan dengan mengikuti prosedur integritas data.
b. Pemeriksaan : tahap ini bertujuan untuk memproses data konten dan *timestamp* dari aplikasi TikTok yang dikumpulkan secara forensik menggunakan berbagai skenario, baik otomatis maupun secara manual, menilai dan merilis data sesuai kebutuhan dengan tetap mengikuti prosedur integritas data.
c. Analisis : tahap ini bertujuan untuk menganalisis hasil pemeriksaan dengan menggunakan metode yang sudah ditentukan secara teknis dan hukum untuk memperoleh informasi yang berguna dan menjawab pertanyaan yang mendorong pengumpulan dan pemeriksaan.
d. Pelaporan : Tahap ini bertujuan untuk melaporkan hasil analisis yang meliputi uraian tindakan yang harus dilakukan, penentuan tindakan yang perlu dilakukan (misalnya pemeriksaan forensik sumber data, celah keamanan yang teridentifikasi, atau peningkatan kontrol keamanan), dan memberikan rekomendasi untuk meningkatkan kebijakan, prosedur, dan aspek lain dari proses forensik.[10]

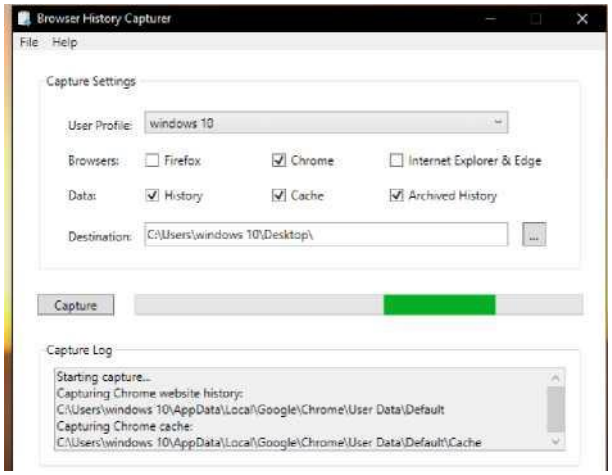
3. HASIL DAN PEMBAHASAN

Aplikasi TikTok ini memberikan akses video, *soundtrack*, akun, dan beberapa informasi lain tanpa harus mendaftarkan akun terlebih dahulu. Tidak seperti *platform* media sosial lainnya, konten di dalam TikTok tidak ditampilkan dalam urutan kronologis karena memiliki algoritma yang diaktifkan untuk menunjukkan informasi akun, berdasarkan jumlah *likes* dan *comments*. Hal ini disebabkan karena atribut dari konten video yang diunggah lebih sulit diidentifikasi.

Pengumpulan data pada penelitian ini dilakukan pada bulan Oktober 2021 dengan menggunakan salah satu unggahan konten video seorang *tiktokers* yang bisa dilihat secara publik tanpa penyelidikan lebih lanjut terkait *timestamp* dari unggahan di bagian konten video tersebut.

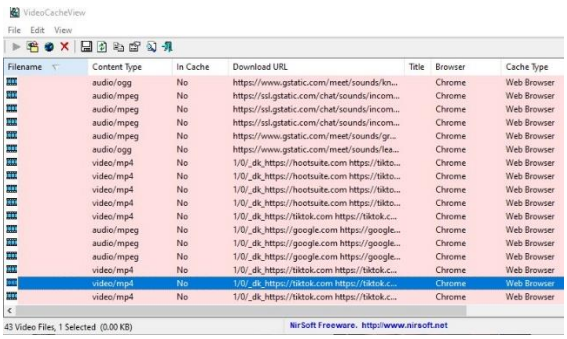
Akuisisi data konten diawali dengan menggunakan *tool Browser History Capture* pada *browser Chrome*, untuk mengambil data dari *browser*. Data yang

dapat diperoleh dari akuisisi *browser* antara lain *history, cache*, dan *archived history*. Aplikasi ini mempunyai beberapa kelebihan dan beberapa kekurangan. Kelebihannya adalah *tool* ini tidak perlu di-*install* pada perangkat sehingga dapat mempercepat proses pendataan. Untuk kekurangannya *tool* ini hanya dapat berjalan pada beberapa aplikasi yaitu pada *Firefox, Chrome*, dan *Internet Explorer & Edge*. Pada folder *history* terdapat beberapa file seperti *Bookmarks, Cookies, Current Session, History, Last session, Login Data, Preferences, Top sites*, dan *Web data*. File di atas akan dianalisis menggunakan *tool Browser History Viewer*. Tahapan akuisisi dengan *tool Browser History Capture* dapat dilihat pada gambar di bawah ini,



Gambar 3. Menampilkan Gambar

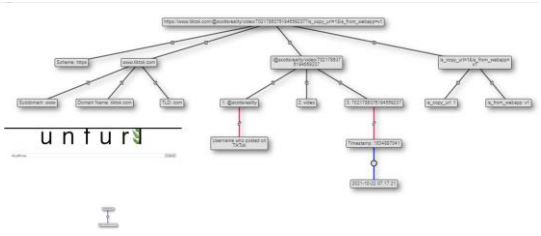
Proses analisis selanjutnya menggunakan *tool Video Cache Viewer* yang digunakan untuk memperoleh video dari aplikasi *browser* seperti *Firefox, Edge*, dan *Chrome*. Proses akuisisi melibatkan ekstraksi file video dari *cache video* di *browser*. Secara otomatis semua cache dari *browser* yang berupa video akan terbaca pada *tool* ini. Saat *tool* ini dibuka, maka akan langsung melakukan proses akuisisi data video pada semua *browser* yang ada. Saat *tool* menyelesaikan akuisisi, akan muncul semua hasil video yang diperoleh dari berbagai sumber. Proses akuisisi dapat dilihat pada gambar di bawah ini,



Gambar 4. Menampilkan Gambar

Proses analisis dari pengumpulan informasi potensial untuk proses identifikasi dari unggahan konten video yang didapatkan dalam salah satu *tiktokers*. Sebagai contoh unggahan video yang diambil orang dengan pengikut cukup banyak di TikTok, @scottsreality dan akan kita analisis dengan menggunakan salah satu *tool* yaitu unfurl.

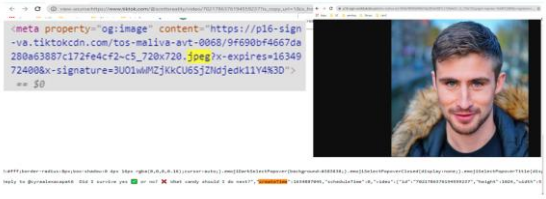
Analisis dengan *tool* unfurl digunakan untuk melihat *timestamp* dari salah satu unggahan video dengan memasukkan *ID createTime*. Pendeteksian *ID createTime* menghasilkan tanggal dan waktu ketika video itu diunggah.



Gambar 5. Tampilan *ID createTime* pada unfurl

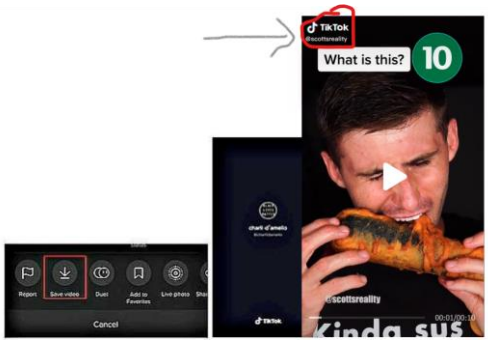
Tampak pada unggahan konten video yang didapatkan dari URL yang dilakukan pada https://www.tiktok.com/@scottsreality/video/7021786376194559237?is_copy_url=1&is_from_webapp=v1 tersebut bahwa konten video itu diunggah pada 22 Oktober 2021 pukul 07:17:21 oleh sang pemilik akun. Informasi *timestamp* yang lain juga dapat diakses dengan mudah melalui

Source Page Link. Gambar profil yang berukuran penuh ataupun gambar yang sudah dipotong bisa ditemukan dengan link yang diberikan oleh URL TikTok. Pencarian *timestamp* gambar ini didapatkan dari *source page link* dengan format .jpeg. Ukuran gambar yang ditemukan adalah yang berukuran 100x100 atau 720x720. Jika diketemukan dengan format 100x100, berarti file tesebut sudah dimanipulasi dari 720x720 ke 100x100 sehingga akan memberikan hasil *output* gambar yang asli yang lengkap seperti gambar di bawah ini.



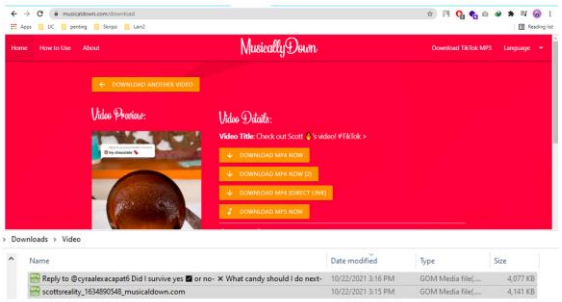
Gambar 6. Menampilkan Gambar Hasil *Output* dari *Source Page Link*

Aplikasi Tiktok ini juga menyediakan fitur untuk menyimpan video yang sudah diunggah, video yang diundauh dalam kondisi yang utuh, atau sebagian adanya dengan *watermark* dari logo tiktok dan *username author* TikTok di layar unggahan video.



Gambar 7. Menampilkan Watermark dari Unggahan Video TikTok

Ternyata untuk penyimpan video tanpa pemakaian *watermark* TikTok dan *username author* TikTok dengan menggunakan tool aplikasi untuk mendapatkan unggahan video tanpa ada *watermark* dengan mengakses laman https://musicallydown.com sehingga terlihat perbedaan antara video unduhan menggunakan aplikasi tiktok dengan *watermark*-nya dan aplikasi yang lain.



Gambar 8. Menampilkan unggahan dari video TikTok tanpa *watermark*

Analisis selanjutnya adalah penemuan *username* TikTok yang dapat disalahgunakan oleh pengguna di TikTok seolah-olah diintimidasi dengan membuat video yang tidak disukai banyak orang. Banyak dari kasus ini langsung dilaporkan dan di-*blacklist* oleh TikTok, tetapi beberapa oknum membuatnya kembali ke *platform* TikTok atau bahkan menghapus videonya dengan mengubah *username* dan memulai dengan akun yang baru. Akun Tiktok dapat mengubah *username* setiap 30 hari, akantetapi, secara teknis setiap bulan atau lebih orang dapat mengubah *username* ke kata kunci yang lain yang tersedia.

Salah satu *tool* yang digunakan yaitu aplikasi https://urlebird.com yang dapat memeriksa dengan cepat apakah ada perubahan *username* dalam waktu dekat ini. Namun, aplikasi ini tidak bisa melacak hingga ke video pertama yang diposting tetapi jauh lebih mudah untuk menggulir video dan memeriksa beberapa bulan terakhir. Banyak *username* yang dibuat dengan cepat saat membuat akun sehingga orang cenderung mengubahnya beberapa hari kemudian ke yang lain. Jika orang tersebut telah memposting video selama

perubahan itu, kedua nama pengguna dapat diperoleh, jika tidak maka tidak akan diketahui oleh orang lain.

Gambar 9. Contoh Tracing Username TikTok yang Telah Diubah

Username dapat mengungkapkan beberapa informasi terkait identitas dari pemilik akun seperti, nama lengkap, tempat dan tanggal lahir atau tahun kelahiran. Dalam contoh di atas, pengguna tersebut memiliki tiga perubahan nama *username* dalam tiga bulan terakhir. Dua di antaranya diubah berdasarkan pada video yang diunggah sehingga mengungkapkan kecenderungan kepribadiannya. Berdasarkan tanggal, memposting dengan *username* itu, sehingga secara jelas bisa diketahui kapan orang tersebut membuat perubahan itu. Perubahan ini tidak mudah diakses di aplikasi *mobile* dan dari situlah kebanyakan orang berasal. Ini bisa menjadi informasi yang terbukti penting untuk beberapa penyelidikan terutama ketika mereka berurusan dengan akun anonim.

TikTok juga memiliki kekurangan seperti setiap *platform* lainnya bahkan lebih menjadi sorotan. Namun, untuk penyelidikan dengan pendekatan OSINT ini adalah tambahan informasi yang bagus yang mungkin tidak ditemukan di tempat lain. Aplikasi TikTok ini dapat memberikan detail pribadi, tempat kerja, rumah alamat dan banyak lainnya, rincian sebagian besar diungkapkan oleh pengguna sendiri.

4. SIMPULAN

Pesatnya perkembangan popularitas aplikasi TikTok menjadikannya sebagai sumber data yang potensial dan berguna untuk forensik digital. Proses analisis untuk menemukan timestamp ini di aplikasi TikTok menggunakan pendekatan metodologi OSINT dan NIST memberikan rekomendasi untuk meningkatkan kebijakan dan prosedur untuk memakai aplikasi TikTok. Hasil percobaan telah membuktikan kemampuan menggunakan konten video dan *timestamp* yang dikumpulkan untuk merekonstruksi *timestamp* dan mencari kata kunci dari pesan yang telah dipertukarkan oleh pengguna di aplikasi TikTok ini.

DAFTAR PUSTAKA

[1] Raluca Matei. (2020) IEEEtran homepage on CTAN. [Online]. Available: https://bloq.hootsuite.com/tiktok-stats/
[2] Faizal Javier. (2020) homepage on Tempo. [Online]. Available: https://data.tempo.co/data/1230/tembus-1-miliar-pengguna-tiktok-hanya-butuh-5-tahun
[3] E. D. S. Watie, “Komunikasi dan Media Sosial (Communications and Social Media),” *J. Messenger*, vol. 3, no. 2, p. 69, 2016.
[4] R. N. Fitriyah, B. Diklat, dan K. Semarang, “Prosiding SENDI _ U 2019 ISBN : 978-979-3649-99-3 Prosiding SENDI _ U 2019 ISBN : 978-979-3649-99-3,” no. 1, pp. 978–979, 2019.
[5] A. Yudhana, I. Riadi, and I. Anshori, “Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist,” It J. Res. Dev., vol. 3, no. 1, p. 13, 2018.
[6] M. N. Fadillah, R. Umar, and A. Yudhana, “Rancangan Metode Nist Untuk Forensik Aplikasi,” Semin.

Nas. Inform. 2018 (semnasIF 2018) UPN "Veteran" Yogyakarta, 24 Novemb. 2018 ISSN 1979-2328, vol. 2018, no. November, pp. 115–119, 2018.

[7] T. R. Afriluyanto, "Fenomena Remaja Menggunakan Media Sosial dalam Membentuk Identitas," *KOMUNIKA J. Dakwah dan Komun*., vol. 11, no. 2, pp. 184–197, 2018.

[8] F. A. Awan, "Forensic examination of social networking applications on smartphones," in 2015 *Conference on Information Assurance and Cyber Security (CIACS),* 2015.

[9] H. D. Karen Kent, Suzanne Chevalier, Tim Grance, "Guide to integrating forensic techniques into incident response (NIST Special Publication 800-86)," NIST Spec. Publ., no. August, pp. 800–886, 2006.

[10] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Analisis Recovery Bukti Digital Instagram Messangers Menggunakan Metode National Institute of Standards and Technology (Nist)," *Semin. Nas. Teknol. Inf. dan Komun. - Semant.,* pp. 161–166, 2017.