

DAFTAR PUSTAKA

- APJII. (2022, Juni). *Profil Internet Indonesia 2022*. Diambil kembali dari Asosiasi Penyedia Jasa Internet Indonesia: <https://apjii.or.id/survei2022x>
- Brown, N. (t.thn.). *Overlay Filesystem*. Diambil kembali dari The Linux Kernel: <https://www.kernel.org/doc/html/latest/filesystems/overlayfs.html?highlight=overlayfs>)
- BSSN. (2021). *Laporan Tahunan Monitoring Keamanan Siber 2021*. Diambil kembali dari Badan Siber dan Sandi Negara: <https://bssn.go.id/publikasi/>
- BSSN. (2022). *Lanskap Keamanan Siber Indonesia*. Jakarta: Direktorat Operasi Keamanan Siber, Badan Siber dan Sandi Negara.
- BSSN. (t.thn.). *Panduan Menghadapi Insiden Data Breach*. Diambil kembali dari Badan Siber dan Sandi Negara: <https://cloud.bssn.go.id/s/QKwjMjJ4rwoneJ9>
- Casey, E. (2004). *Digital Evidence and Computer Crime*. Great Britain: ACADEMIC PRESS.
- Ciardhuáin, S. Ó. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence* .
- Cloudflare. (t.thn.). *What is a computer port? | Ports in networking*. Diambil kembali dari Cloudflare: <https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/>
- CNN Indonesia. (2019, Februari 7). *225 Juta Serangan Siber Masuk Indonesia Sepanjang 2018*. Diambil kembali dari CNN Indonesia: <https://www.cnnindonesia.com/teknologi/20190207210646-185-367347/225-juta-serangan-siber-masuk-indonesia-sepanjang-2018>
- Cooper, C. (2018, Mei 16). *Wanna Cry: Lessons Learned 1 Year Later*. Diambil kembali dari Symantec: <https://www.symantec.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later>
- Cyberthreat.id. (2020, Oktober 20). *Puslabfor Bareskrim Polri Ungkap 8 Tantangan Forensik Digital*. Diambil kembali dari Cyberthreat.id:

<https://cyberthreat.id/read/8897/Puslabfor-Bareskrim-Polri-Ungkap-8-Tantangan-Forensik-Digital>

Denholm, T. (2018). *Explaining OverlayFS – What it Does and How it Works*. Diambil kembali dari Datalight: <https://www.datalight.com/blog/2016/01/27/explaining-overlayfs-%E2%80%93-what-it-does-and-how-it-works/>

EC-Council. (2009). *Computer Hacking Forensics Investigator Version 3*.

Google. (t.thn.). *Introduction to robots.txt*. Diambil kembali dari Google Search Central: <https://developers.google.com/search/docs/advanced/robots/intro>

Ieong, R. S.-C. (2006). FORZA: Digital Forensics Investigation Framework. *Digital Forensic Research Conference*. Lafayette.

IETF. (2006, Januari). *The Secure Shell (SSH) Protocol Architecture*. Diambil kembali dari Internet Engineering Task Force: <https://datatracker.ietf.org/doc/html/rfc4251>

IETF. (2009, Maret). *The Syslog Protocol*. Diambil kembali dari IETF : <https://datatracker.ietf.org/doc/html/rfc5424>

Jansen, W., & Ayers, R. (2004). *Guidelines on PDA Forensics*. Gaithersburg: National Institute of Standards and Technology.

Kaspersky. (2019, November). *Cyberthreat Real-Time Map*. Diambil kembali dari Kaspersky: <https://cybermap.kaspersky.com/stats/#country=144&type=ids&period=m>

Kircaali, Y. C. (2020, Januari 3). *Typhoon: 1.02 Vulnhub Walkthrough*. Diambil kembali dari Yucel Can Kircaali: <https://www.yckircaali.com/typhoon-1-02-vulnhub-walkthrough/>

Kompas.com. (2021, Mei 22). *Kronologi Kasus Kebocoran Data WNI, Dijual 0,15 Bitcoin hingga Pemanggilan Direksi BPJS*. Diambil kembali dari Kompas.com: <https://tekno.kompas.com/read/2021/05/22/09450057/kronologi-kasus-kebocoran-data-wni-dijual-0-15-bitcoin-hingga-pemanggilan>

Liputan6. (2019). *Bagaimana Kondisi Keamanan Siber di Indonesia selama Kuartal Kedua 2019?* Diambil kembali dari Liputan6: <https://cybermap.kaspersky.com/>

NIST. (2015). Secure Hash Standard (SHS). *FIPS PUB 180-4*, 8.

- NIST. (t.thn.). *DIGITAL EVIDENCE*. Diambil kembali dari NIST: <https://www.nist.gov/digital-evidence#:~:text=Digital%20forensics%20is%20the%20field,and%20other%20data%20storage%20devices>.
- O'Reilly and Associates. (2001). *Managing System Logs*. Diambil kembali dari Running Linux Third Edition: https://docstore.mik.ua/oreilly/linux/run/ch08_03.htm
- Pandora FMS. (2021, Agustus 27). *Log Monitoring: What should we do before we start?* Diambil kembali dari Pandora FMS: <https://pandorafms.com/blog/log-monitoring/>
- PortSwigger. (t.thn.). *Clickjacking (UI redressing)*. Diambil kembali dari PortSwigger: <https://portswigger.net/web-security/clickjacking>
- PortSwigger. (t.thn.). *Cross-site scripting*. Diambil kembali dari PortSwigger: <https://portswigger.net/web-security/cross-site-scripting>
- Primartha, R. (2018). *Security Jaringan Berbasis CEH*. Bandung: Penerbit INFORMATIKA.
- Riza, H., Darmawan, D., Utoyo, I., Lahey, T., Izza, J., Lim, E., . . . Usino, W. (2020). *Data and Cyber Security*. Jakarta Selatan: Perkumpulan Basis Data Indonesia.
- Scientific Working Group on Digital Evidence. (2000, April). *Forensics Science Communications*. Diambil kembali dari FBI: <https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm>
- Tech Terms. (2008, April 16). *Disk Image*. Diambil kembali dari Tech Terms.com: <https://techterms.com/definition/diskimage>
- The Next Web. (2017, Mei 15). *How one guy stopped the WannaCry ransomware in its tracks after it spread to 150 countries*. Diambil kembali dari The Next Web: <https://thenextweb.com/security/2017/05/15/how-one-guy-stopped-the-wannacry-ransomware-in-its-tracks-after-it-spread-to-150-countries/>
- Ubuntu. (2015, Juni 15). *CVE-2015-1328*. Diambil kembali dari Ubuntu: <https://ubuntu.com/security/CVE-2015-1328>

Webopedia. (2006, Februari 28). *Image*. Diambil kembali dari Webopedia:
<https://www.webopedia.com/definitions/image/>