

## DAFTAR PUSTAKA

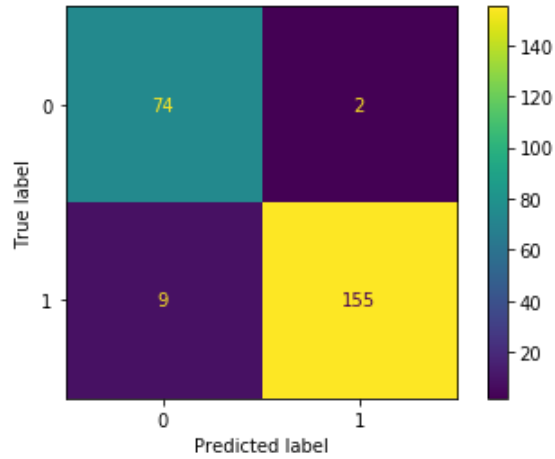
- Adamu, U., & Awan, I. (2019). Ransomware Prediction Using Supervised Learning Algorithms. *IEEE Access*, 57–63.  
<https://doi.org/10.1109/Ficloud.2019.00016>
- Agcaoili, J., Ang, M., Earnshaw, E., Gelera, B., & Tamana, N. (N.D.). Ransomware Double Extortion And Beyond: Revil, Clop, And Conti. 1–23.  
<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti>
- Ahmed, Y. A., Koçer, B., & Al-Rimy, B. A. S. (2020). Automated Analysis Approach For The Detection Of High Survivable Ransomware. *KSII Transactions On Internet And Information Systems*, 14(5), 2236–2257.  
<https://doi.org/10.3837/tiis.2020.05.021>
- Al-Rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2019). Crypto-Ransomware Early Detection Model Using Novel Incremental Bagging With Enhanced Semi-Random Subspace Selection. *Future Generation Computer Systems*, 101, 476–491. <https://doi.org/10.1016/j.future.2019.06.005>
- Al Bakri, Abbas M, Hussein, H. L. (2014). Static Analysis Based Behavioral API For Malware Detection Using Markov Chain. *Computer Engineering And Intelligent Systems*, 5(12).
- Al, S., & Cau, A. (2012). Behavioural API Based Virus Analysis And Detection. *IJCSIS) International Journal Of Computer Science And Information Security*, 10(5), 5500.
- Ali, M., Shiaeles, S., Bendiab, G., & Ghita, B. (2020). Malgra: Machine Learning And N-GRAM Malware Feature Extraction And Detection System. *Electronics (Switzerland)*, 9(11), 1–20.  
<https://doi.org/10.3390/electronics9111777>
- Ashraf, A., Aziz, A., Zahoor, U., & Khan, A. (2019). Ransomware Analysis Using Feature Engineering And Deep Neural Networks. 1–15.  
<http://arxiv.org/abs/1910.00286>
- Bahrani, A., & Bidgly, A. J. (2019). Ransomware Detection Using Process Mining And Classification Algorithms. *Proceedings Of 16th International ISC Conference On Information Security And Cryptology, ISCISC 2019, Iscisc*, 73–77. <https://doi.org/10.1109/ISCISC48546.2019.8985149>
- Bajpai, P., & Enbody, R. (2020). An Empirical Study Of API Calls In Ransomware. *IEEE International Conference On Electro Information Technology*, 2020-July, 443–448.  
<https://doi.org/10.1109/EIT48999.2020.9208284>
- Canzanese, R., Mancoridis, S., & Kam, M. (2016). Run-Time Classification Of Malicious Processes Using System Call Analysis. *2015 10th International Conference On Malicious And Unwanted Software, MALWARE 2015*, October, 21–28. <https://doi.org/10.1109/MALWARE.2015.7413681>
- Casaseca-De-La-Higuera, P., Martín-Fernández, M., & Alberola-López, C.

- (2006). Weaning From Mechanical Ventilation: A Retrospective Analysis Leading To A Multimodal Perspective. *IEEE Transactions On Biomedical Engineering*, 53(7), 1330–1345.  
<https://doi.org/10.1109/TBME.2006.873695>
- Chen, Z. G., Kang, H. S., Yin, S. N., & Kim, S. R. (2017). Automatic Ransomware Detection And Analysis Based On Dynamic API Calls Flow Graph. *Proceedings Of The 2017 Research In Adaptive And Convergent Systems, RACS 2017, 2017-Janua*, 196–201.  
<https://doi.org/10.1145/3129676.3129704>
- Coplin, W. M., Pierson, D. J., Cooley, K. D., Newell, D. W., & Rubinfeld, G. D. (2000). Implications Of Extubation Delay In Brain-Injured Patients Meeting Standard Weaning Criteria. *American Journal Of Respiratory And Critical Care Medicine*, 161(5), 1530–1536.  
<https://doi.org/10.1164/Ajrcm.161.5.9905102>
- Egunjobi, S., Parkinson, S., & Crampton, A. (2019). Classifying Ransomware Using Machine Learning Algorithms. *Lecture Notes In Computer Science (Including Subseries Lecture Notes In Artificial Intelligence And Lecture Notes In Bioinformatics)*, 11872 LNCS(December), 45–52.  
[https://doi.org/10.1007/978-3-030-33617-2\\_5](https://doi.org/10.1007/978-3-030-33617-2_5)
- Fang, Y., Zeng, Y., Li, B., Liu, L., & Zhang, L. (2020). Deepdetectnet Vs Rlattacknet: An Adversarial Method To Improve Deep Learningbased Static Malware Detection Model. In *Plos ONE (Vol. 15, Issue 4)*.  
<https://doi.org/10.1371/Journal.Pone.0231626>
- Hakim, A. A., Erwin, A., Eng, K. I., Galinium, M., & Muliady, W. (2014). Automated Document Classification For News Article In Bahasa Indonesia Based On Term Frequency Inverse Document Frequency (TF-IDF) Approach. *Proceedings - 2014 6th International Conference On Information Technology And Electrical Engineering: Leveraging Research And Technology Through University-Industry Collaboration, ICITEE 2014*, 0–3.  
<https://doi.org/10.1109/ICITEED.2014.7007894>
- Harjono. (2013). Menggunakan Dionaee ( Malware Detection In The Network Using Dionaee ) Harjono. *Techno*, 14(2), 64–69.
- Hwang, J., Kim, J., Lee, S., & Kim, K. (2020). Two-Stage Ransomware Detection Using Dynamic Analysis And Machine Learning Techniques. *Wireless Personal Communications*, 112(4), 2597–2609.  
<https://doi.org/10.1007/S11277-020-07166-9>
- Maniath, S., Ashok, A., Poornachandran, P., & Jan, S. (2017). Deep Learning Lstm Based Ransomware Detection. 3.
- Mariconti, E., Onwuzurike, L., Andriotis, P., De Cristofaro, E., Ross, G., & Stringhini, G. (2017). Mamadroid: Detecting Android Malware By Building Markov Chains Of Behavioral Models. *IEEE Access*, Ndss.  
<https://doi.org/10.14722/Ndss.2017.23353>
- Nguyen, D. T., & Lee, S. (2021). Lightgbm-Based Ransomware Detection Using API Call Sequences. *International Journal Of Advanced Computer Science And Applications*, 12(10), 138–146.  
<https://doi.org/10.14569/IJACSA.2021.0121016>

- Ninyesiga, A., & Ngubiri, J. (2018). Malware Classification Using API System Calls. *International Journal Of Technology And Management*, 3(2).  
<https://Utamu.Ac.Ug/Ijotm/Index.Php/Ijotm/Article/View/41>
- Nurnoby, M. F., & El-Alfy, E. S. M. (2019). Overview And Case Study For Ransomware Classification Using Deep Neural Network. 2019 2nd IEEE Middle East And North Africa Communications Conference, Menacomm 2019. <https://doi.org/10.1109/Menacomm46666.2019.8988551>
- Qin, B., Wang, Y., & Ma, C. (2020). API Call Based Ransomware Dynamic Detection Approach Using Textcnn. *Proceedings - 2020 International Conference On Big Data, Artificial Intelligence And Internet Of Things Engineering, ICBAIE 2020*, 162–166.  
<https://doi.org/10.1109/ICBAIE49996.2020.00041>
- Ruwali, A., Kumar, A. J. S., Prakash, K. B., Sivavaraprasad, G., & Ratnam, D. V. (2021). Implementation Of Hybrid Deep Learning Model (LSTM-CNN) For Ionospheric TEC Forecasting Using GPS Data. *IEEE Geoscience And Remote Sensing Letters*, 18(6), 1004–1008.  
<https://doi.org/10.1109/LGRS.2020.2992633>
- Schofield, M., Alicioglu, G., Binaco, R., Turner, P., Thatcher, C., Lam, A., & Sun, B. (2021). Convolutional Neural Network For Malware Classification Based On API Call Sequence. *Computer Science & Information Technology (CS & IT)*, 85–98. <https://doi.org/10.5121/Csit.2021.110106>
- Seifert, C., Steenson, R., Welch, I., Komisarczuk, P., & Endicott-Popovsky, B. (2007). Capture - A Behavioral Analysis Tool For Applications And Documents. *Digital Investigation*, 4(SUPPL.), 23–30.  
<https://doi.org/10.1016/J.Diin.2007.06.003>
- Sheen, S., & Yadav, A. (2018). Ransomware Detection By Mining API Call Usage. 2018 International Conference On Advances In Computing, Communications And Informatics, ICACCI 2018, 983–987.  
<https://doi.org/10.1109/ICACCI.2018.8554938>
- Syaputra, R. (2020). Studi Literatur Analisis Malware Menggunakan Metode Analisis Dinamis Dan Statis. *Jurnal Jaringan Komputer Dan Keamanan*, 1(1), 14–24.
- Tran, T. K., & Sato, H. (2017). NLP-Based Approaches For Malware Classification From API Sequences. *Proceedings - 2017 21st Asia Pacific Symposium On Intelligent And Evolutionary Systems, IES 2017, 2017-Janua*, 101–105.
- Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A Survey On Trust Management For Internet Of Things. *Journal Of Network And Computer Applications*, 42, 120–134. <https://doi.org/10.1016/J.Jnca.2014.01.014>
- Zhou, J., Hirose, M., Kakizaki, Y., & Inomata, A. (2020). Evaluation To Classify Ransomware Variants Based On Correlations Between Apis. *ICISSP 2020 - Proceedings Of The 6th International Conference On Information Systems Security And Privacy, Icissp 2020*, 465–472.  
<https://doi.org/10.5220/0008959904650472>

# LAMPIRAN

### Lampiran 1 *Confusion Matrix* Untuk Pembelajaran Model Dataset 1

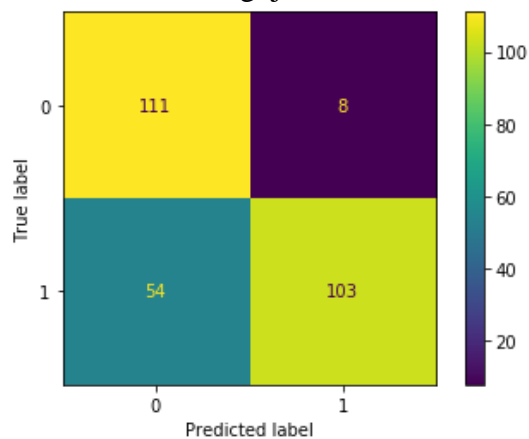


### Lampiran 2 Hasil Top Fitur SVM Dataset 1

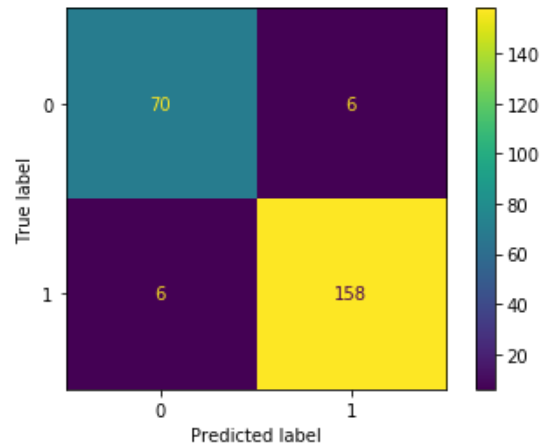
**y=Ransomware** top features

Weight <sup>2</sup>	Feature
+9.028	__exception__
+6.593	rtidecompressbuffer
+5.082	ntopenkey setfilepointer
+5.033	ldrunloaddll ntreadfile
+4.503	findresourcea
+4.353	ntreadfile ldrgetdllhandle
+3.896	createprocessinternalw ntqueryvaluekey
+3.764	getnativesysteminfo
+3.077	sizeofresource createactctxw
+2.723	ntcreatefile getsystemtimeasfiletime
+2.641	ntreadfile
+2.573	ntclose ldrunloaddll
+2.506	ntdelayexecution
+2.409	getsysteminfo

### Lampiran 3 *Confusion Matrix* SVM Pengujian Model Data Varian Baru Dataset 1



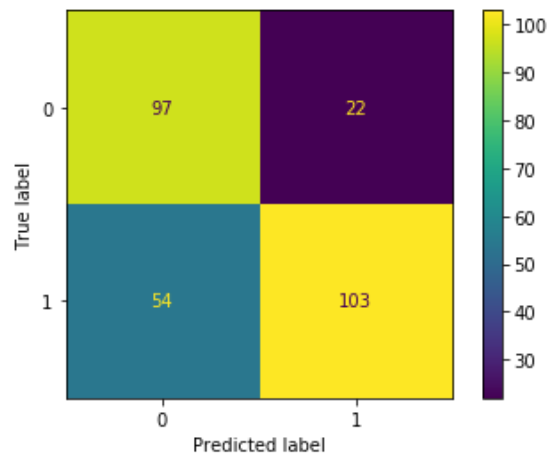
#### Lampiran 4 *Confusion Matrix* Random Forest Untuk Pembelajaran Model Dataset 1



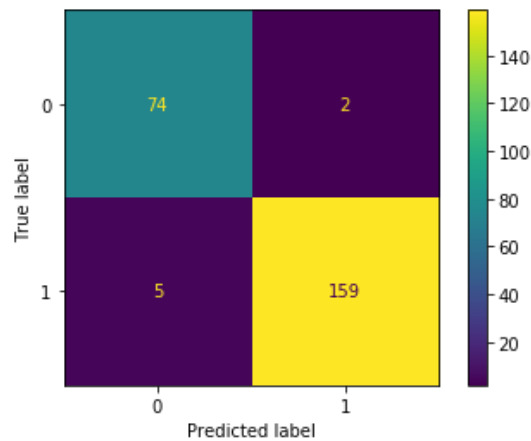
#### Lampiran 5 Hasil Top Fitur Random Forest Dataset 1

Weight	Feature
0.0208 ± 0.1165	ldrloaddll nterminateprocess
0.0176 ± 0.0794	setunhandledexceptionfilter
0.0174 ± 0.0974	getnativesysteminfo
0.0146 ± 0.0979	setunhandledexceptionfilter seterrormode
0.0144 ± 0.0558	ntreadfile
0.0143 ± 0.0984	getsystemtimeasfiletime ldrloaddll
0.0143 ± 0.0868	ntdelayexecution
0.0127 ± 0.0869	lookupprivilegevaluew
0.0108 ± 0.0801	seterrormode ntcreatefile
0.0105 ± 0.0777	ntclose getsystemtimeasfiletime
0.0105 ± 0.0551	setunhandledexceptionfilter findresourceexw
0.0094 ± 0.0378	ntcreatefile
0.0094 ± 0.0769	nterminateprocess getfileattributesw
0.0089 ± 0.0712	getusernameexw
0.0089 ± 0.0600	createactctxw
0.0088 ± 0.0720	ntwritefile

#### Lampiran 6 *Confusion Matrix* RF Pengujian Model Data Varian Baru Dataset 1



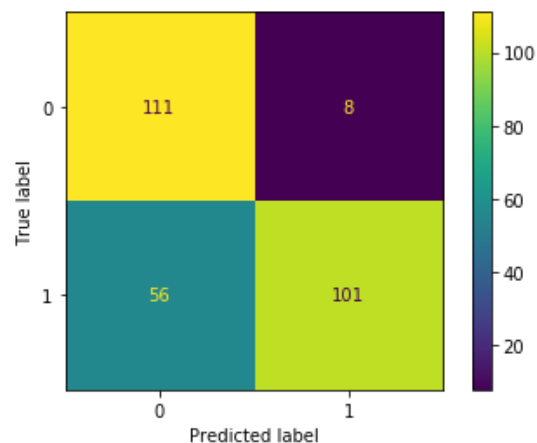
**Lampiran 7** *Confusion Matrix* LightGBM Untuk Pembelajaran Model Dataset 1



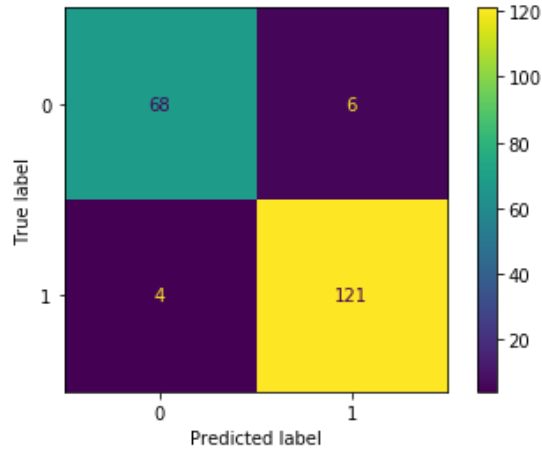
**Lampiran 8** Hasil Top Fitur LightGBM Dataset 1

Weight	Feature
0.1201	setunhandledexceptionfilter
0.1168	getnativesysteminfo
0.0559	lookupprivilegevaluew
0.0477	ldrloaddll ntterminateprocess
0.0383	ntdelayexecution
0.0379	ntcreatefile
0.0346	getsystemdirectoryw regenumkeyexw
0.0308	writeconsolew
0.0257	ntprotectvirtualmemory
0.0188	ntduplicateobject ntopensection
0.0179	__exception__
0.0178	getusernameexw
0.0149	ntprotectvirtualmemory coinitalizeex
0.0148	createactctxw
0.0143	ntqueryvaluekey getfileattributesw
0.0141	findresourcea

**Lampiran 9** *Confusion Matrix* LightGBM Pengujian Model dengan Data Varian Baru Dataset 1



**Lampiran 10** *Confusion Matrix* SVM Pembelajaran Model Dataset 2

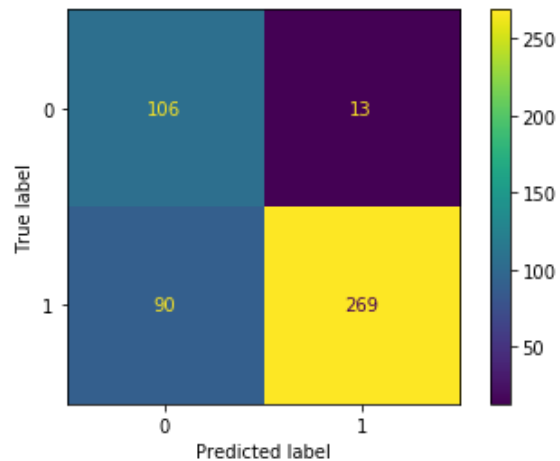


**Lampiran 11** Hasil Top Fitur SVM Dataset 2

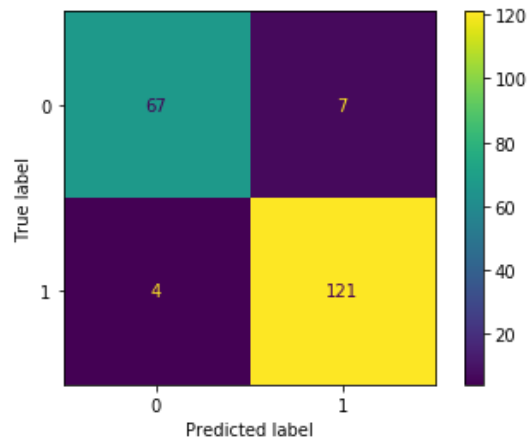
**y=Ransomware** top features

Weight <sup>2</sup>	Feature
+3.580	ldrloaddll ntallocatevirtualmemory
+1.746	ntallocatevirtualmemory createactctxw
+1.497	ntprotectvirtualmemory
+1.389	__exception__
+1.365	ntfreevirtualmemory ntprotectvirtualmemory
+1.307	findresourcea
+1.221	ntquerysysteminformation ntreadfile
+1.119	coinitializesecurity isdebuggerpresent
+1.103	searchpathw ntopenkey
+1.100	wsastartup
+1.088	cryptacquirecontextw
+1.051	writeconsolew
+1.025	getnativesysteminfo ntopensection
+1.007	ntdelayexecution
+0.945	findfirstfileexw ntcreatesection
+0.944	ldrgetdllhandle ntopenkey

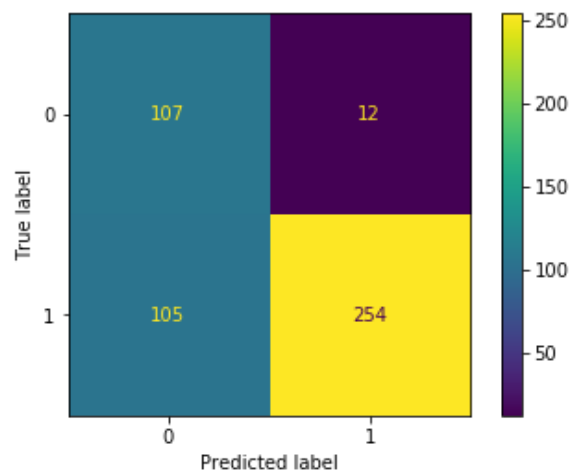
**Lampiran 12** *Confusion Matrix* SVM Pengujian Model dengan Data Varian Baru Dataset 2



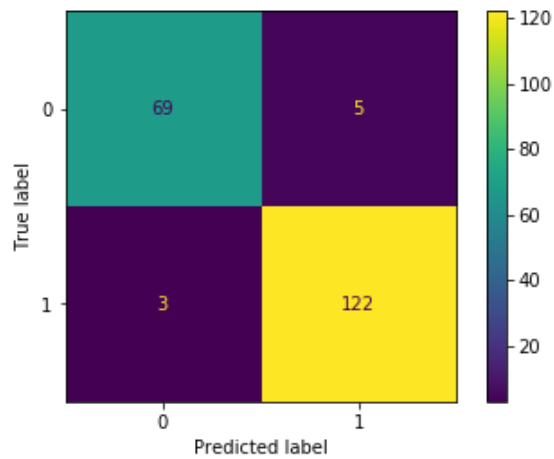


**Lampiran 13** *Confusion Matrix* Random Forest Pembelajaran Model Dataset 2**Lampiran 14** Hasil Top Fitur Random Forest Dataset 2

Weight	Feature
0.0225 ± 0.1271	ldrloaddll ntterminateprocess
0.0218 ± 0.1020	setunhandleexceptionfilter
0.0211 ± 0.1350	getnativesysteminfo
0.0180 ± 0.1272	regqueryvalueexa
0.0154 ± 0.0881	loadstringw
0.0138 ± 0.0921	createactctxw
0.0134 ± 0.0960	ntcreatefile ntclose
0.0132 ± 0.0942	createactctxw ntopenkey
0.0127 ± 0.0914	seterrormode ntcreatefile
0.0124 ± 0.1022	regsetvalueexw
0.0115 ± 0.0854	ntterminateprocess getfileattributesw
0.0104 ± 0.0768	ntdelayexecution
0.0104 ± 0.0720	ldrgetdllhandle
0.0102 ± 0.0885	regopenkeyexa
0.0102 ± 0.0854	ntwritefile

**Lampiran 15** *Confusion Matrix* Random Forest Pengujian Model dengan Data Varian Baru Dataset 2

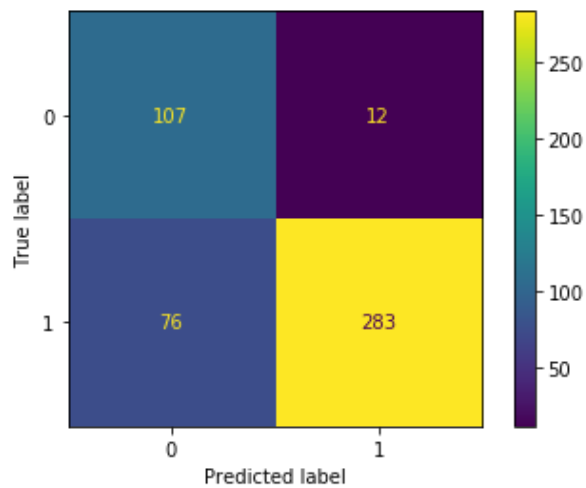
**Lampiran 16** *Confusion Matrix* LightGBM Untuk Pembelajaran Model Dataset 2



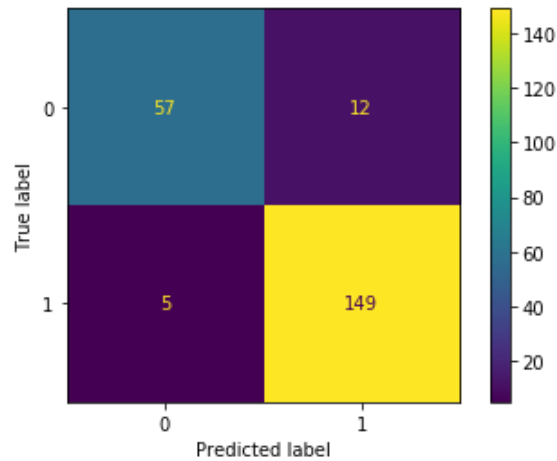
**Lampiran 17** Hasil Top Fitur LightGBM Dataset 2

Weight	Feature
0.1201	setunhandleexceptionfilter
0.1142	getnativesysteminfo
0.0653	ldrloaddll nterminateprocess
0.0568	regqueryvalueexa
0.0424	ntduplicateobject ntopensection
0.0377	lookupprivilegevaluw
0.0338	ntprotectvirtualmemory
0.0333	createactcbw
0.0297	ntfreevirtualmemory ntprotectvirtualmemory
0.0244	ntcreatesection loadstringw
0.0233	loadstringw
0.0227	ntdelayexecution
0.0190	__exception__
0.0143	isdebuggerpresent
0.0128	writeconsolew

**Lampiran 18** *Confusion Matrix* LightGBM Pengujian Model dengan Data Varian Baru Dataset 2



**Lampiran 19** *Confusion Matrix* SVM Untuk Pembelajaran Model Dataset 3

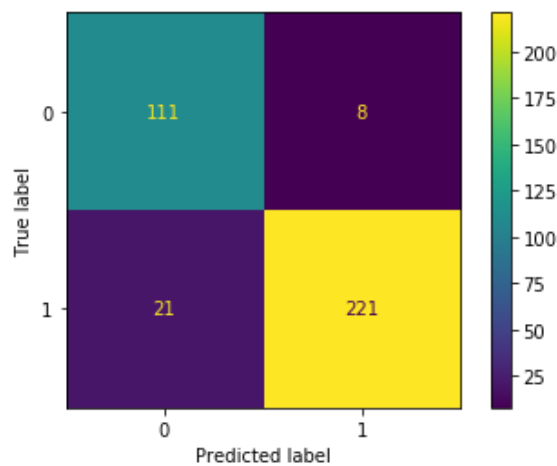


**Lampiran 20** Hasil Top Fitur SVM Dataset 3

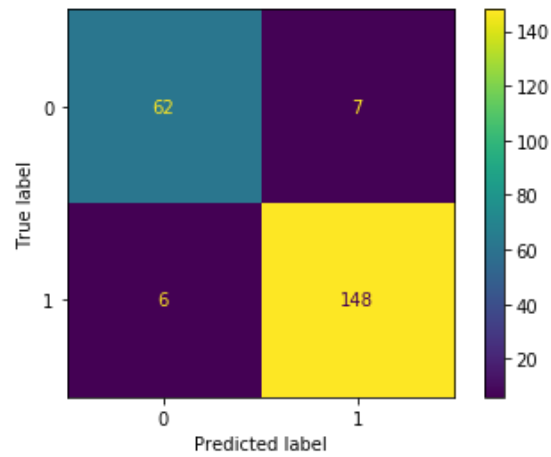
**y=Ransomware** top features

Weight?	Feature
+7.091	__exception__
+5.706	ntallocatevirtualmemory createactctxw
+3.666	ntreadfile ldrgetdllhandle
+3.420	ntcreatesection loadstringw
+3.173	loadstringw ldrgetprocedureaddress
+2.724	seterrormode ntreadfile
+2.597	findresourcea
+2.552	ntprotectvirtualmemory
+2.547	ntfreevirtualmemory ntprotectvirtualmemory
+2.192	globalmemorystatusex closesocket
+2.156	getsystemtimeasfiletime ntcreatesection
+2.081	lookupprivilegevaluw
+2.051	ntcreatefile getsystemtimeasfiletime
+1.966	ntopenkey ldrgetprocedureaddress
+1.957	ntclose getfileattributesw
+1.883	ntopenfile loadstringa
+1.869	ntreadfile

**Lampiran 21** *Confusion Matrix* SVM Pengujian Model dengan Data Varian Baru Dataset 3



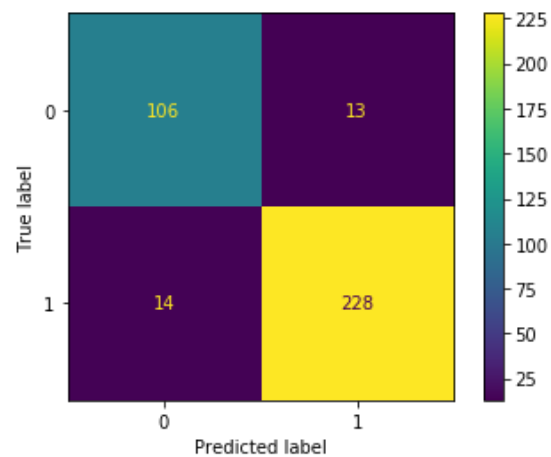
**Lampiran 22** *Confusion Matrix* Random Forest Pembelajaran Model Dataset 3



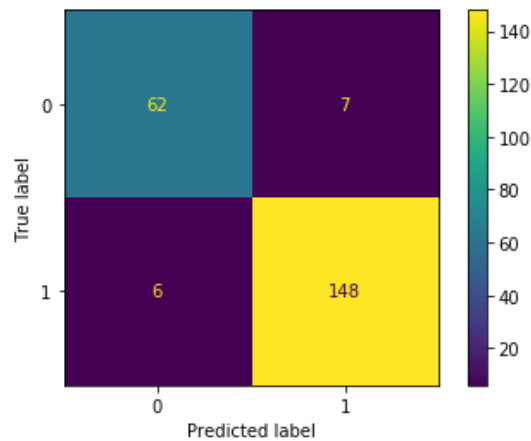
**Lampiran 23** Hasil Top Fitur Random *Forest* Dataset 3

Weight	Feature
0.0225 ± 0.1150	ntdelayexecution
0.0193 ± 0.0959	ldrloaddll ntterminateprocess
0.0190 ± 0.0843	setunhandledexceptionfilter
0.0132 ± 0.0614	ntallocatevirtualmemory ldrgetdllhandle
0.0128 ± 0.0776	getnativesysteminfo
0.0109 ± 0.0692	seterrormode ntcreatefile
0.0108 ± 0.0832	ntwritefile
0.0108 ± 0.0690	ntterminateprocess getfileattributesw
0.0106 ± 0.0703	createactctxw ntopenkey
0.0104 ± 0.0529	loadstringw
0.0102 ± 0.0447	ntreadfile
0.0100 ± 0.0633	ntcreatefile ntclose
0.0098 ± 0.0729	ntdelayexecution seterrormode
0.0096 ± 0.0777	regsetvalueexw
0.0092 ± 0.0732	ntqueryinformationfile
0.0089 ± 0.0708	lookupprivilegevaluw
0.0087 ± 0.0420	ntprotectvirtualmemory

**Lampiran 24** *Confusion Matrix* Random Forest Pengujian Model Data Varian Baru Dataset 3



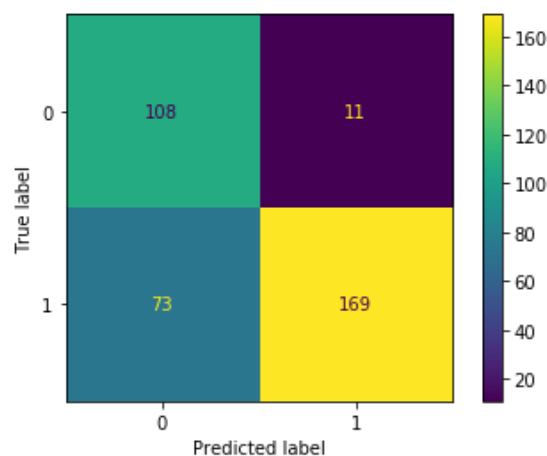
### Lampiran 25 Confusion Matrix LightGBM Pembelajaran Model Dataset 3



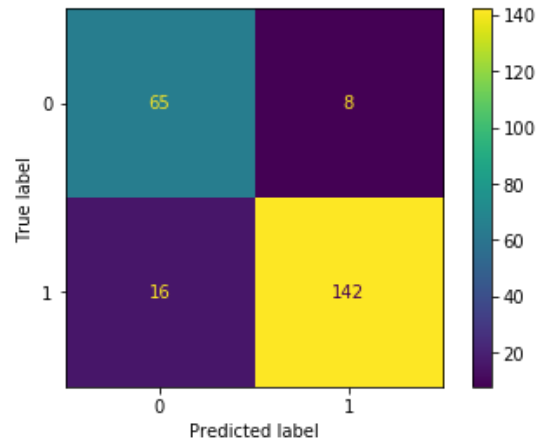
### Lampiran 26 Hasil Top Fitur LightGBM Dataset 3

Weight	Feature
0.1707	ntdelayexecution
0.0492	ntreadfile
0.0389	getvolumenameforvolumemountpointw
0.0382	getsystemdirectoryw regenumkeyexw
0.0342	setunhandledexceptionfilter
0.0341	lookupprivilegevaluw
0.0309	findresourcea
0.0297	ntprotectvirtualmemory
0.0263	createprocessinternalw
0.0225	createactcbw
0.0211	ntqueryinformationfile writeconsolew
0.0201	process32nextw
0.0189	ntqueryattributesfile ntcreatmutant
0.0180	loadstringw ldrgetprocedureaddress
0.0165	ntopenkey ntfreevirtualmemory
0.0161	certcontrolstore
0.0143	setunhandledexceptionfilter seterrormode
0.0126	__exception__

### Lampiran 27 Confusion Matrix LightGBM Pengujian Model dengan Data Varian Baru Dataset 3



**Lampiran 28** Confusion Matrix SVM Pembelajaran Model Dataset 4

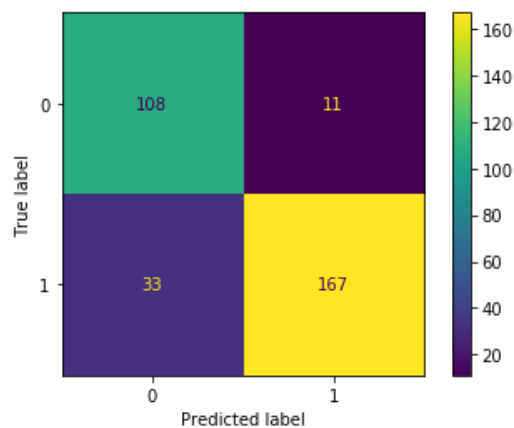


**Lampiran 29** Hasil Top Fitur SVM Dataset 4

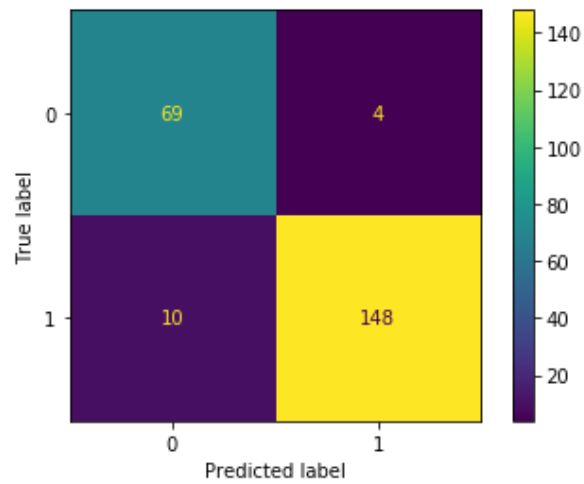
**y=Ransomware top features**

Weight <sup>2</sup>	Feature
+17.068	rtldecompressbuffer
+10.063	getsystemtimeasfiletime ldrloaddll
+9.749	ntcreatesection loadstringw
+8.139	__exception__
+7.801	ntprotectvirtualmemory
+7.044	ntopenkey setfilepointer
+6.916	ldrunloaddll ntreadfile
+6.270	ntqueryvaluekey ntqueryvaluekey
+6.230	ntfreevirtualmemory ntprotectvirtualmemory
+5.447	createprocessinternalw ntqueryvaluekey
+5.370	ntfreevirtualmemory ldrloaddll
+5.290	findresourcea
+5.106	ntprotectvirtualmemory ldrloaddll
+4.898	ntmapviewofsection ldrloaddll
+4.107	createactcbw ntopenkey
+3.935	ntdelayexecution

**Lampiran 30** Confusion Matrix SVM Pengujian Model dengan Data Varian Baru Dataset 4



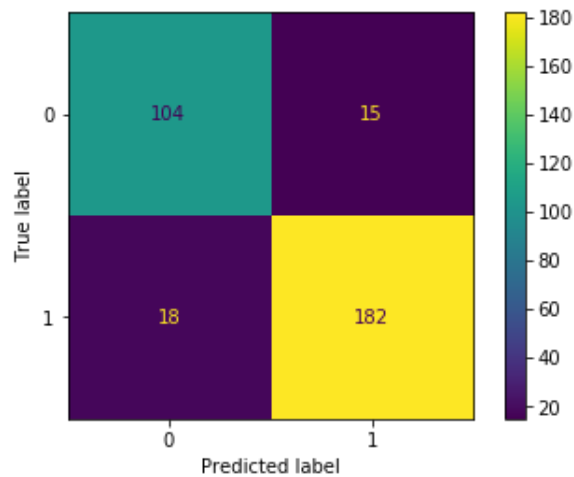
**Lampiran 31** *Confusion Matrix* Random Forest Pembelajaran Model Dataset 4



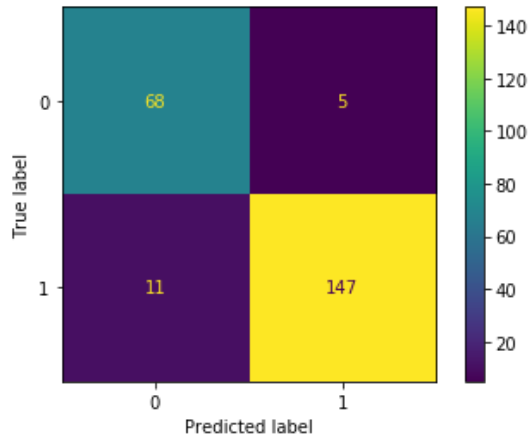
**Lampiran 32** Hasil Top Fitur Random Forest Dataset 4

Weight	Feature
0.0173 ± 0.0637	setunhandledexceptionfilter
0.0169 ± 0.0844	ldrloaddll nterminateprocess
0.0156 ± 0.1122	getusernameexw
0.0133 ± 0.0521	ntreadfile
0.0120 ± 0.0859	lookupprivilegevaluw
0.0116 ± 0.0814	getnativesysteminfo
0.0115 ± 0.0644	ldrgetprocedureaddress
0.0112 ± 0.0637	ntcreatefile ntclose
0.0108 ± 0.0638	seterrormode ntcreatefile
0.0103 ± 0.0848	ntopenprocess getfileattributesw
0.0100 ± 0.0826	cocreateinstance ntunmapviewofsection
0.0098 ± 0.0620	ntcreatesection loadstringw
0.0094 ± 0.0549	ntdelayexecution
0.0091 ± 0.0526	ldrgetdllhandle
0.0090 ± 0.0434	loadstringw

**Lampiran 33** Hasil *Confusion Matrix* Random Forest Pengujian Model Untuk Data Varian Baru Dataset 4



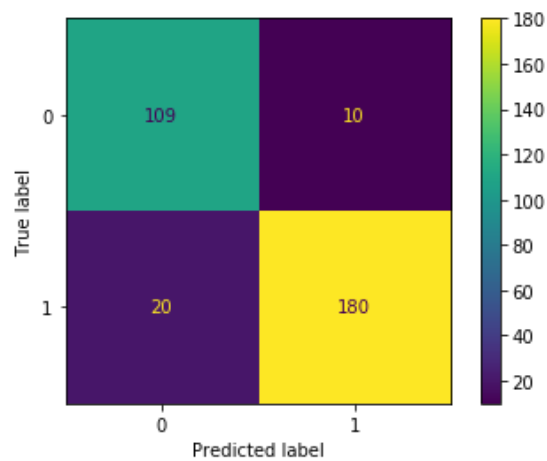
**Lampiran 34** *Confusion Matrix* LightGBM Pembelajaran Model Dataset 4



**Lampiran 35** Hasil Top Fitur LightGBM Dataset 4

Weight	Feature
0.1567	getusernameexw
0.1002	setunhandledexceptionfilter
0.0825	lookupprivilegevaluw
0.0607	writeconsolew
0.0335	ntreadfile
0.0297	setfilepointer
0.0286	__exception__
0.0276	ntcreatefile
0.0208	ldrloaddll ntterminateprocess
0.0190	ntdelayexecution
0.0178	ntopenkey ntfreevirtualmemory
0.0147	loadstringw
0.0146	ntclose
0.0144	createactctxw
0.0142	getnativesysteminfo
0.0133	ntcreatefile ntclose
0.0126	closesocket

**Lampiran 36** *Confusion Matrix* LightGBM Pengujian Model Untuk Data Varian Baru Dataset 4





**Lampiran 37** Kesamaan Fitur Setiap Model Pada Seluruh Dataset

Kesamaan Fitur Dataset 1		Kesamaan Fitur Dataset 2		Kesamaan Fitur Dataset 3		Kesamaan Fitur Dataset 4	
__exception__	getforegroundwindow ntquerykey	getnativesysteminfo	oleinitialize	ntdelayexecution	ntquerysysteminformation ntresumethread	rtldecompressbuffer	ntenumeratevaluekey
rtldecompressbuffer	ldrgetprocedureaddress ntopenthread	regqueryvalueexa	getfiletype	ntreadfile	ldrgetprocedureaddress ntenumeratekey	getsystemtimeasfiletime ldrloaddll	regopenkeyexa ldrgetdllhandle
findresourcea	findfirstfileexw ntcreatemutant	regsetvalueexw	ntcreatesection ntopenkey	getvolumenameforvolumemountpointw	getfileinformationbyhandleex ldrgetdllhandle	ntcreatesection loadstringw	ntterminateprocess ntqueryvaluekey
createprocessinternalw ntqueryvaluekey	writeprocessmemory	ntdelayexecution	ldrloaddll ntallocatevirtualmemory	lookupprivilegevaluew	gettimezoneinformation	__exception__	coinitializeex
getnativesysteminfo	createdirectoryw deletefilew	ldrgetdllhandle	findresourcea	findresourcea	ldrgetdllhandle ntcreatesection	ntprotectvirtualmemory	oleinitialize
ntcreatefile getsystemtimeasfiletime	cocreateinstance	regopenkeyexa	createtoolhelp32snapshot	ntprotectvirtualmemory	loadstringw ntopenkey	ntqueryvaluekey ntqueryvaluekey	ntallocatevirtualmemory regopenkeyexa
ntreadfile	loadresource	lookupprivilegevaluew	ldrgetdllhandle ntopenkey	createprocessinternalw	ntreadfile ntopenfile	ntfreevirtualmemory ntprotectvirtualmemory	readprocessmemory
ntdelayexecution	loadstringw ntopenkey	ldrgetprocedureaddress	ntqueryinformationfile	ntqueryinformationfile writeconsolew	socket regsetvalueexw	createprocessinternalw ntqueryvaluekey	shgetfolderpathw
getsysteminfo	ntopenkey	ntprotectvirtualmemory	coinitializesecurity	process32nextw	ntquerysysteminformation ntsetvaluekey	ntfreevirtualmemory ldrloaddll	regsetvalueexa
ntprotectvirtualmemory shgetfolderpathw	messageboxtimeoutw	getusernameexw	deletefilew	loadstringw ldrgetprocedureaddress	ntopenkeyex ldrloaddll	findresourcea	cogetclassobject

Kesamaan Fitur Dataset 1		Kesamaan Fitur Dataset 2		Kesamaan Fitur Dataset 3		Kesamaan Fitur Dataset 4	
ntquerysysteminformation ntreadfile	lookupaccountsidw	createprocessinternalw	ntopenkey ntfreevirtualmemory	ntopenkey ntfreevirtualmemory	ntopenthread getfiletype	createactctxw ntopenkey	socket
wsastartup getsystemwindowsd irectoryw	regenumkeyexa	ntduplicateobject	regopenkeyexw	__exception__	cryptacquirecontextw	ntdelayexecution	ntqueryinformationfile
ntsetcontextthread	ntreadfile ntopenfile	ntcreatefile	ldrgetprocedureaddress ntenumeratekey	ldrloaddll ntqueryinformationfile	ntopenkey ldrgetprocedureaddress	sizeofresource createactctxw	cocreateinstance ntunmapviewofsection
lookupprivilegevaluew	getsystemmetrics ntcreatethreadex	writeconsolew	getsysteminfo	ntopenfile loadstringa	regopenkeyexw	loadstringw ldrgetprocedureaddress	getfileattributesw ntfreevirtualmemory
ntopenfile loadstringa	regopenkeyexa ldrgetdllhandle	ntallocatevirtualmemory	ntresumethread	regqueryvalueexa wsastartup	ntopenkeyex	lookupprivilegevaluew	getsysteminfo regqueryvalueexa
ntqueryvaluekey getnativesysteminfo	ntclose getsystemtimeasfiletime	ldrloaddll	loadstringw ldrgetprocedureaddress	seterrormode ntallocatevirtualmemory	ntprotectvirtualmemory ldrloaddll	ntpendirectoryobject	ntduplicateobject regclosekey
messageboxtimeoutw setunhandledexceptionfilter	ldrgetdllhandle ntcreatesection	closesocket	ntqueryvaluekey ldrloaddll	rtladdvectoredexceptionhandler	searchpathw	createactctxw regopenkeyexw	regopenkeyexw
ldrloaddll couninitialize	ntpendirectoryobject ldrloaddll	ntopenkey	cogetclassobject	setfilepointer	ntpendirectoryobject	ldrgetprocedureaddress ldrloaddll	seterrormode ntallocatevirtualmemory
ntfreevirtualmemory ldrloaddll	createthread ntunmapviewofsection	socket	ntopenprocess getfileattributesw	ntqueryinformationfile	getsystemtimeasfiletime findfirstfileexw	ntcreatefile getsystemtimeasfiletime	ntallocatevirtualmemory createactctxw
ntcreatesection loadstringw	getusernameexw	ntpendirectoryobject	oleinitialize ntopenfile	getfilesizeex createthread	ntquerysysteminformation	ntclose getfileattributesw	regsetvalueexw ntopenkey

Kesamaan Fitur Dataset 1		Kesamaan Fitur Dataset 2		Kesamaan Fitur Dataset 3		Kesamaan Fitur Dataset 4	
ntpendirectoryobject	ntquerysysteminformation	process32nextw	ntopenkeyldrgetprocedureaddress	drawtextexw	regopenkeyexadeletefilew	ntopenkeyntfreevirtualmemory	regclosekeyntreadfile
wsastartup	getsystemmetricscreateactctxw	ntclose	ntenumeratevaluekey	getfilesize	ntdelayexecutionseterrormode	getshortpathnamew	closesocket
regsetvalueexa	ntterminateprocessuידcreate	ntreadfile	regsetvalueexa	ntcreatefile	writeprocessmemory	ntquerysysteminformation	ntprotectvirtualmemorycoinitializeex
sizeofresource	getsystemmetrics	ntterminateprocess	ntallocatevirtualmemoryregopenkeyexa	socket	coinitializeexntcreatesection	ntopenkey	getvolumenameforvolumemountpointw
cocreateinstance regenumkeyexw	getfileattributesw	findfirstfileexw	copyfilew	findfirstfileexw	findfirstfileexw closesocket	ldrgetdllhandle ntfreevirtualmemory	ntopenprocess getfileattributesw
findfirstfileexw ntcreatesection	createdirectoryw	ntdelayexecution seterrormode	createthread	ntreadfile ldrgetdllhandle	getforegroundwindow	ntopenkey ldrgetprocedure address	getbestinterfaceex ldrloaddll
ntopenthread getfiletype	ntmapviewofsection	wsastartup	setfiletime	getfilesize regopenkeyexw	couninitialize regclosekey	ntmapviewofsection getsystemmetrics	regqueryvalueexa
regenumkeyexw cryptacquirecontextw	crypthashdata	ntcreatefile getsystemtimeasfile time	regenumkeyw	getshortpathnamew	ntclose getfileattributesw	wsastartup	ntterminateprocess
createactctxw ntopenkey	findresourceexw ntcreatefile	regclosekey	ntprotectvirtualmemory shgetfolderpathw	ntfreevirtualmemory ntprotectvirtualmemory	getfilesizeex	seterrormode ntreadfile	regqueryvalueexw
createprocessinternalw	gettempfilepathw	cocreateinstance	getfiletype ldrloaddll	ldrgetdllhandle	cocreateinstance regenumkeyexw	ntopenfile loadstringa	ntcreatemutant ntprotectvirtualmemory

Kesamaan Fitur Dataset 1		Kesamaan Fitur Dataset 2		Kesamaan Fitur Dataset 3		Kesamaan Fitur Dataset 4	
findfirstfileexw	ntallocatevirtualmemory	ntfreevirtualmemory ntprotectvirtualmemory	setwindowshookexa	loadstringa	regcreatekeyexa regqueryvalueexw	loadstringa	getsystemtimeasfiletime cointializeex
getshortpathnamew	ntwritefile	__exception__	cryptacquirecontxtw	ntallocatevirtualmemory	ntallocatevirtualmemory regopenkeyexa	sizeofresource	getusernameexw
getsystemtimeasfiletime ldrloaddll	regcreatekeyexa	ntfreevirtualmemory	getsystemwindow sdirectoryw ntclose	wsastartup	regqueryvalueexw ntfreevirtualmemory	ntqueryvaluekey	ntenumeratekey
ntcreatethreadex	regqueryvalueexa wsastartup	ntopenkey ntopenmutant	createdirectoryw	deviceiocontrol	regcreatekeyexa	getsystemdirect orya	ntsetcontextthread
deletefilew ldrgetdllhandle	getfileinformationbyh andleex ldrgetdllhandle	getnativesysteminfo ntopensection	getsystemtimeasfi letime findfirstfileexw	getsysteminfo	crypthashdata	ldrgetprocedure address ntenumeratekey	ntresumethread getfilesizeex
ntcreatekey	ntresumethread	ldrloaddll getsysteminfo	cointializeex	ntallocatevirtualme mory createactctw	getsysteminfo regqueryvalueexa	ldrloaddll ntqueryinformat ionfile	ntqueryvaluekey regqueryvalueexw
getsystemtimeasfile time findfirstfileexw	ntterminateprocess ntqueryvaluekey	gettimezoneinforma tion	readprocessmemo ry	regqueryvalueexw ntmapviewofsection	loadstringw findresourceexw	ntterminateproc ess getfileattribes w	ldrgetdllhandle ntallocatevirtualmem ory
closesocket	writeconsolew ntqueryvaluekey	writeconsolew ntclose	ntqueryinformatio nfile writeconsolew	ldrloaddll	getusernamew	setfilepointer ntquerydirectory file	setfilepointer
searchpathw	ntqueryvaluekey regcreatekeyexa	getsystemmetrics ntmapviewofsection	ntopenmutant ldrgetproceduread dress	ldrgetdllhandle ntfreevirtualmemor y	ntprotectvirtualmemory cointializeex	ntreadfile ntduplicateobjec t	ntprotectvirtualmemo ry shgetfolderpathw
getvolumepathname w	ntclose	ntqueryvaluekey ntqueryvaluekey	regcreatekeyexw	oleinitialize	setunhandledexceptionf ilter ntopenkey	ldrloaddll couninitialize	ntcreatesection

Kesamaan Fitur Dataset 1		Kesamaan Fitur Dataset 2		Kesamaan Fitur Dataset 3		Kesamaan Fitur Dataset 4	
process32nextw	ntduplicateobject	cocreateinstance regenumkeyexw	ntquerysysteminf ormation ntreadfile	regclosekey	ntcreatethreadex	regenumkeyexw loadstringw	ntdelayexecution seterrormode
regopenkeyexa ntwritefile	ntenumeratevaluekey	getbestinterfaceex ldrloaddll	ntenumeratekey	ntresumethread	ntqueryvaluekey ntduplicateobject	getfilesizeex createthread	ldrloaddll ntterminateprocess
loadstringw findresourceexw	regopenkeyexw	regsetvalueexw ntopenkey	ntcreatemutant ntprotectvirtualme mory	ntcreatefile getsystemtimeasfile time	ntmapviewofsection ldrloaddll	socket regsetvalueexw	ntreadfile
getvolumenameforv olumemountpointw	ntqueryvaluekey getfileattributesw	ntenumeratekey getfiletype	ntallocatevirtualm emory ldrgetdllhandle	ldrloaddll ntqueryvaluekey	findfirstfileexw ntcreatemutant	regclosekey	wsastartup ntterminateprocess
getsystemtimeasfile time coinitializeex	getsysteminfo regqueryvalueexa	ldrgetprocedureaddr ess ldrloaddll	ntterminateproces s writeconsolew	ntcreatemutant ntprotectvirtualme mory	ntduplicateobject regclosekey	writeconsolew	findfirstfileexw ntcreatesection
ntcreatesection ntopenkey	ntcreatethreadex regopenkeyexw	ntprotectvirtualme mory ldrloaddll	coinitializesecurit y getfiletype	setfileattributesw	coinitializeex cocreateinstance	ntquerydirectory file	regopenkeyexw seterrormode
ldrloaddll ntqueryvaluekey	coinitializeex regenumvaluew	getsystemtimeasfile time getcomputernamea	ntduplicateobject regclosekey	ntenumeratevalueke y	createactctxw ntopenkey	findfirstfileexw	ntopenmutant loadresource
ntcreatefile	deletefilew	cocreateinstanceex ntduplicateobject	sizeofresource	ldrgetdllhandle ntopenkey	ntqueryinformationfile createprocessinternalw	ntresumethread	getsystemtimeasfileti me findfirstfileexw
ntfreevirtualmemor y ntquerysysteminfor mation	ntterminateprocess writeconsolew	wsastartup getsystemwindowssd irectoryw	getcomputername a	findresourceexw ntcreatefile	ntopenfile setfilepointer	findfirstfileexw ntcreatemutant	regqueryinfokeyw cocreateinstance
setfilepointer setunhandledexcept ionfilter	ldrloaddll	ntclose ntmapviewofsection	rtldecompressbuff er	getsystemwindowssd irectoryw ntqueryvaluekey	ntquerykey regqueryvalueexa	regopenkeyexa ntwritefile	writeprocessmemory
writeconsolew	regqueryvalueexw ntmapviewofsection	ntunmapviewofsecti on	ntallocatevirtualm emory createactctxw	ntclose	regqueryvalueexw	getfileinformati onbyhandleex ldrgetdllhandle	ntcreatefile

Kesamaan Fitur Dataset 1		Kesamaan Fitur Dataset 2		Kesamaan Fitur Dataset 3		Kesamaan Fitur Dataset 4	
		getsystemdirectoryw					
loadstringw ldrgetprocedureaddress	createthread	createdirectoryw deletefilew	searchpathw ntopenkey	createprocessinternalw ntqueryvaluekey	coinitializeex	ntpendirectoryobject ldrloaddll	getadaptersinfo
setfilepointer	couninitialize regclosekey	getkeystate	getkeystate getcursorpos	ldrgetprocedureaddress	ntduplicateobject	ntopenkeyex	netshareenum
getfilesize	createactctxw regopenkeyexw	getcomputernamew setfilepointer	ntcreatethreadex regopenkeyexw	getsystemtimeasfiletime ldrloaddll	ntduplicateobject getsysteminfo	ntopenfile	setendoffile
cryptacquirecontextw	getfileversioninfoexw	regenumvaluea getfiletype	getusernameexw ldrloaddll	regsetvalueexa	closesocket	ntcreatefile getvolumename forvolumemountpointw	deletefilew ntwritefile
deviceiocontrol	rtladdvectoredexceptionhandler	ntsetvaluekey	ldrloaddll ntcreatefile	ntqueryvaluekey ntqueryvaluekey	ntcreatesection	getsystemdirectoryw ntquerydirectoryfile	sendnotifymessagew ntopenprocess
getsystemdirectoryw ccreateinstance	regenumkeyw			getsystemdirectoryw ntquerydirectoryfile	ntopenprocess	ccreateinstanceex	oleinitialize ntopenfile
coinitializeex regdeletevaluew	ntqueryinformationfile			createdirectoryw	createdirectoryw deletefilew	ntquerydirectoryfile loadstringw	ntqueryvaluekey getnativesysteminfo
ntduplicateobject getsysteminfo	ntdelayexecution seterrormode			deletefilew ldrgetdllhandle	writeconsolew	ldrloaddll	gettemppathw ntcreatefile
oleinitialize	ldrgetdllhandle			ntqueryvaluekey ldrloaddll	getsystemtimeasfiletime	unhookwindowshookex	ldrgetprocedureaddress ntopenthread
ntallocatevirtualmemory regopenkeyexa	ntqueryvaluekey ntopenprocess			ntopenkey	regenumvaluew	ntreadfile ntopenfile	ntopensection getforegroundwindow

Kesamaan Fitur Dataset 1		Kesamaan Fitur Dataset 2		Kesamaan Fitur Dataset 3		Kesamaan Fitur Dataset 4	
ntprotectvirtualmemory coinitializeex	ntopensection regclosekey			ntmapviewofsection	ntprotectvirtualmemory shgetfolderpathw	getsystemwindo wsdirectoryw ntqueryvaluekey	createthread getsystemdirectoryw
ntopenprocess	ntresumethread getfilesizeex			regsetvalueexw ntopenkey	regenumkeyexw cryptacquirecontextw	getbestinterfac ex	getkeystate getcursorspos
getsystemtimeasfile time getcomputernamea	ldrloaddll getfileattributesw			deletefilew	regenumkeyw	regopenkeyexw ntdelayexecutio n	regenumkeyexw cryptacquirecontextw
ntwritefile ldrgetdllhandle	ldrloaddll ntqueryinformationfil e			ntwritefile ldrgetdllhandle	ntcreatefile ntclose	ntdeviceiocontr olfile	ntquerydirectoryfile setunhandledexceptio nfilter
ntunmapviewofsecti on regqueryinfokeyw	createactctxw getfilesize				getfileattributesexw	createprocessint ernalw	
ntopenfile	coinitializeex						
ldrgetprocedureaddr ess ldrloaddll	drawtextexw						
couninitialize	ldrgetprocedureaddre ss						
getfilesize regopenkeyexw	ntallocatevirtualmem ory createdirectoryw						
regqueryvalueexw	regenumkeyexw						
createthread getsystemdirectory w	loadstringw createactctxw						
wsastartup ntterminateprocess							



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI  
**UNIVERSITAS HASANUDDIN**  
**FAKULTAS TEKNIK**

Jalan Poros Malino Km. 6 Bontomarannu Gowa, 92171 Sulawesi Selatan

☎ (0411) 586015, 586262 Fax (0411) 586015.

<http://eng.unhas.ac.id>. E-mail: [teknik@unhas.ac.id](mailto:teknik@unhas.ac.id)

**SURAT KEPUTUSAN**  
**DEKAN FAKULTAS TEKNIK UNIVERSITAS HASANUDDIN**  
**NOMOR : 6152 /UN.4.7.1/TD. 06 /2022**  
**TENTANG**  
**PENGANGKATAN KOMISI PENASEHAT TESIS BAGI MAHASISWA PROGRAM MAGISTER**  
**TEKNIK INFORMATIKA DEPARTEMEN INFORMATIKA FAKULTAS TEKNIK**  
**UNIVERSITAS HASANUDDIN**

**DEKAN FAKULTAS TEKNIK UNIVERSITAS HASANUDDIN**

- Membaca** : Surat usulan Ketua Program Studi S2 Teknik Informatika Nomor: 5922 tanggal 25 Maret 2022 perihal Usulan Komisi Penasehat dan Rencana Judul Tesis bagi Sdr. Hartinah
- Menimbang** : a. Bahwa dalam rangka pelaksanaan bimbingan Tesis bagi Sdr. **Hartinah** Nomor Pokok **D082202010** mahasiswa Program Magister Informatika Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin, dipandang perlu mengangkat Komisi Penasehat Tesis;  
b. bahwa untuk keperluan huruf (a) di atas, maka dipandang perlu menerbitkan Surat Keputusan.
- Mengingat** : 1. Keputusan Rektor UNHAS No. 7343/J04/P/2001  
2. Keputusan Rektor UNHAS No. 1067/J04/P/2003  
3. Keputusan Rektor UNHAS No. 824/H4/P/2007

**MEMUTUSKAN**

- Menetapkan** : KEPUTUSAN DEKAN FAKULTAS TEKNIK UNIVERSITAS HASANUDDIN TENTANG PENGANGKATAN KOMISI PENASEHAT TESIS BAGI MAHASISWA PROGRAM MAGISTER TEKNIK INFORMATIKA DEPARTEMEN TEKNIK INFORMATIKA FAKULTAS TEKNIK UNIVERSITAS HASANUDDIN. A.N : Hartinah NOMOR POKOK D082202010
- PERTAMA** : Mengangkat Komisi Penasehat Tesis bagi Sdr. Hartinah Nomor Pokok D082202010 mahasiswa Program Magister Teknik Informatika Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin  
Judul : "Deteksi Klasifikasi Ransomware Berdasarkan Pemanggilan Api Sistem Operasi Windows"  
Dengan susunan sebagai berikut :
1. Penasehat Utama : Dr. Eng. Ady Wahyudi Paundu, ST., MT (Pemb. I)  
2. Penasehat Anggota : Dr. Ir. Amil Ahmad Ilham, ST., M.IT (Pemb.II)
- KEDUA** : Belanja Vakasi/ honorium sebahaimana dimaksud pada diktum pertama, dibebankan pada Dana DPA PTNBH UNHAS Tahun 2022 ( BPPS, dan DIKTI ) Alokasi Fakultas Teknik.
- KETIGA** : Surat Keputusan ini berlaku terhitung mulai tanggal ditetapkan sampai dengan selesainya masa studi yang bersangkutan, dengan ketentuan apabila dikemudian hari ternyata terdapat kesalahan atau kekeliruan didalamnya, akan diadakan perbaikan sebagaimana mestinya.

Ditetapkan di Makassar,

Pada tanggal 29 Maret 2022

a.n. Dekan,

Wakil Dekan Bidang Akademik Riset dan Inovasi

Prof. Ir. Baharuddin Hamzah, ST, M.Arch, Ph.D  
Nip. 19690308 199512 1 001

**Tembusan Yth :**

1. Dekan FT-UH
2. Wakil Dekan II FT-UH
3. Ketua Program Studi S2 Teknik Informatika
4. Sdr. Hartinah
5. Arsip







KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI  
UNIVERSITAS HASANUDDIN  
FAKULTAS TEKNIK

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

Kampus Fakultas Teknik Unhas, Jl. Poros Malino, Gowa  
<http://eng.unhas.ac.id/informatika>, Email : [informatika@unhas.ac.id](mailto:informatika@unhas.ac.id)

Gowa, 25 Maret 2022

Nomor : 5922/UN4.7.8/TD.06/2022  
Lampiran : -  
Hal : Usulan Susunan Komisi Penasehat dan Rencana Judul Tesis

Yth,  
Wakil Dekan Bidang Akademik Riset dan Inovasi  
Fakultas Teknik Unhas  
di-  
Gowa

Dengan hormat,

Dengan ini kami yang bertanda tangan di bawah ini sesuai minat mahasiswa dan hasil rapat kelompok kerja dosen KKD Program Studi S2 kami mengusulkan komisi penasehat tesis bagi saudara :

Nama : Hartinah  
No Pokok : D082202010  
Program Studi : S2 Teknik Informatika

Dengan Rencana Judul Tesis :

**“Deteksi Klasifikasi Ransomware berdasarkan Pemanggilan Api Sistem Operasi Windows”**

Dengan Susunan sebagai berikut :

Penasehat Utama : Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.

Penasehat Anggota : Dr. Ir. Amil Ahmad Ilham, S.T., M.IT

Kami usulkan kiranya dapat diterbitkan surat keputusan. Atas kerjasamanya kami sampaikan terima kasih.

Ketua Program Studi  
Magister Teknik Informatika FT-UH

Dr. Ir. Zahir Zainuddin, M. Sc  
NIP. 19640427 198910 1 002

Tembusan:  
1. Arsip