

2020 JBU-CTF

Forensic
Crypto

문승재

문제목록

Forensic

Trace USB 2.0

600

Crypto

German Army's cipher

700

Forensic

Trace USB

600

Trace USB

600

누군가 나의 PC에 악성 프로그램이 담긴 USB를 꽂아 사용한 것 같다.

해당 USB와 관련된 정보를 다 모으자

Flag = scpCTF{시리얼번호_최초연결시간(월_일_시_분)_드라이브문자}

최초연결시간은 24시 표기법을 사용한다.

USB.egg

scpCTF{...}

Submit

in Army's cipher

700

문제풀이

레지스트리 주요 경로

HKLM\SYSTEM\ControlSet00\Enum\USBSTOR

%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-DriverFrame-works-UserMode%4Operational.evtx

C:\Windows\inf\Setupapi.dev.log

HKLM\SYSTEM\ControlSet00\Enum\WpdBusEnumRoot\UMB

HKLM\SOFTWARE\Microsoft\WindowsPortableDevices\Devices

문제풀이

The screenshot displays a forensic analysis interface with two main panels. The left panel, titled 'Evidence Tree', shows a hierarchical view of a file system. The right panel, titled 'File List', shows a table of files with columns for Name, Size, Type, and Date Modified. A context menu is open over the 'SOFTWARE' file in the File List, showing options: 'Export Files...', 'Export File Hash List...', and 'Add to Custom Content Image (AD1)'.

Evidence Tree

- System32
 - 0409
 - AdvancedInstallers
 - appraiser
 - ar-SA
 - bg-BG
 - Boot
 - catroot
 - catroot2
 - CodeIntegrity
 - com
 - CompatTel
 - config
 - cs-CZ
 - da-DK
 - de-DE
 - Dism
 - drivers
 - DriverStore
 - el-GR
 - en
 - en-US
 - es-ES
 - et-EE
 - fi-FI
 - fr-FR

File List

Name	Size	Type	Date Modified
DEFAULT.LOG1.FileSl...	11	File Slack	
DEFAULT.LOG2	0	Regular File	2009-07-14 ...
SAM	256	Regular File	2020-10-09 ...
SAM.LOG	1	Regular File	2011-12-20 ...
SAM.LOG1	17	Regular File	2020-10-09 ...
SAM.LOG2	0	Regular File	2009-07-14 ...
SECURITY	256	Regular File	2020-10-09 ...
SECURITY.LOG	1	Regular File	2011-12-20 ...
SECURITY.LOG1	21	Regular File	2020-10-09 ...
SECURITY.LOG2	0	Regular File	2009-07-14 ...
SOFTWARE	57,088	Regular File	2020-10-09 ...
SOFTWARE.FileSlack	168	File Slack	
SOFTWARE.LOG	1	Regular File	2011-12-20 ...
SOFTWARE.LOG1	256	Regular File	2020-10-09 ...
SOFTWARE.LOG1.FileSlack	4,608	File Slack	
SOFTWARE.LOG2	0	Regular File	2009-07-14 ...
SYSTEM	12,032	Regular File	2020-10-09 ...
SYSTEM.FileSlack	168	File Slack	
SYSTEM.LOG	1	Regular File	2011-12-20 ...
SYSTEM.LOG1	256	Regular File	2020-10-09 ...
SYSTEM.LOG1.FileSlack	4,608	File Slack	
SYSTEM.LOG2	0	Regular File	2009-07-14 ...

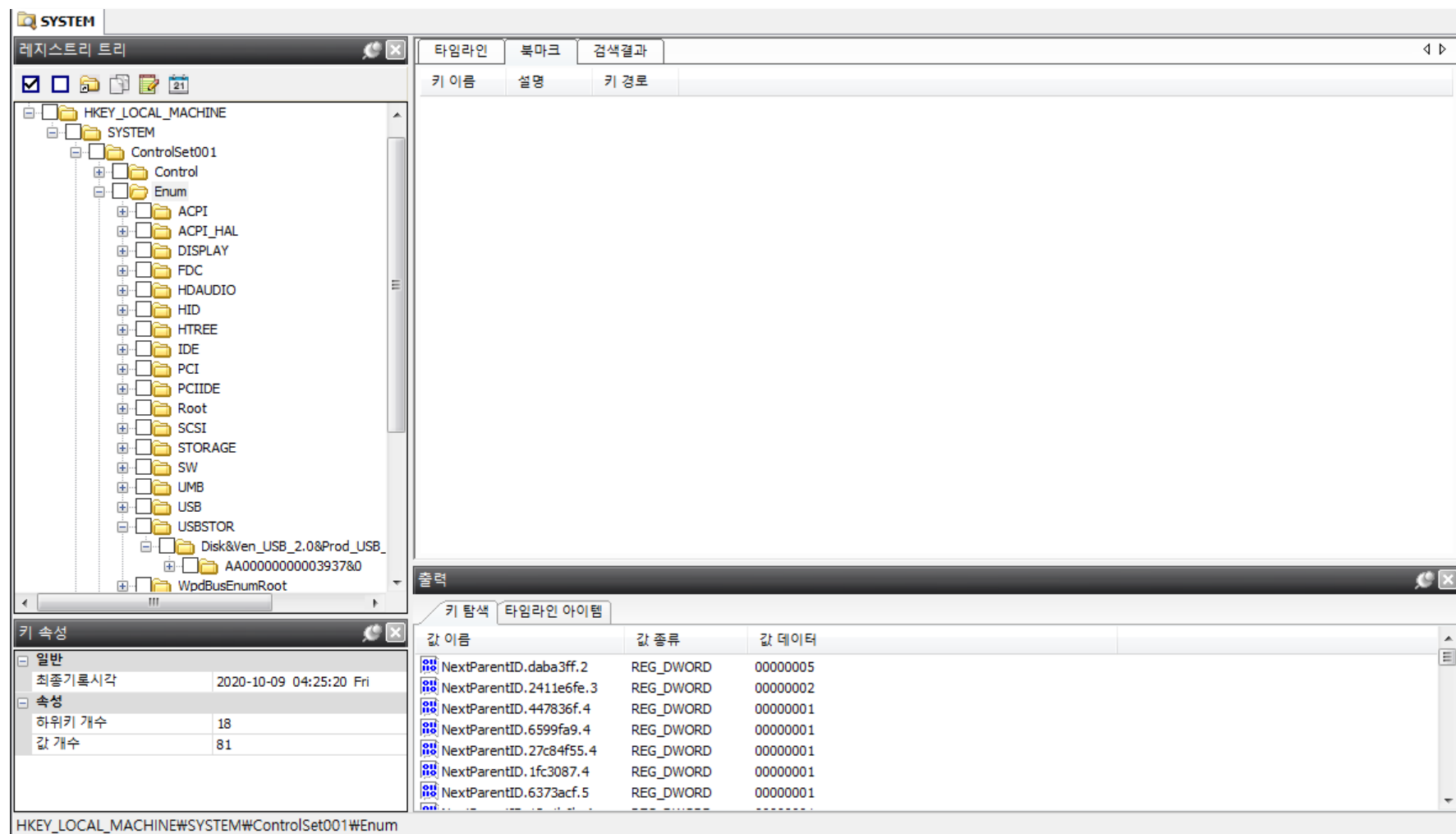
Context Menu Options:

- Export Files...
- Export File Hash List...
- Add to Custom Content Image (AD1)

Evidence Tree Tabs: Evidence Tree | Properties | Hex Value Interpreter | Custom Content Sources

문제풀이

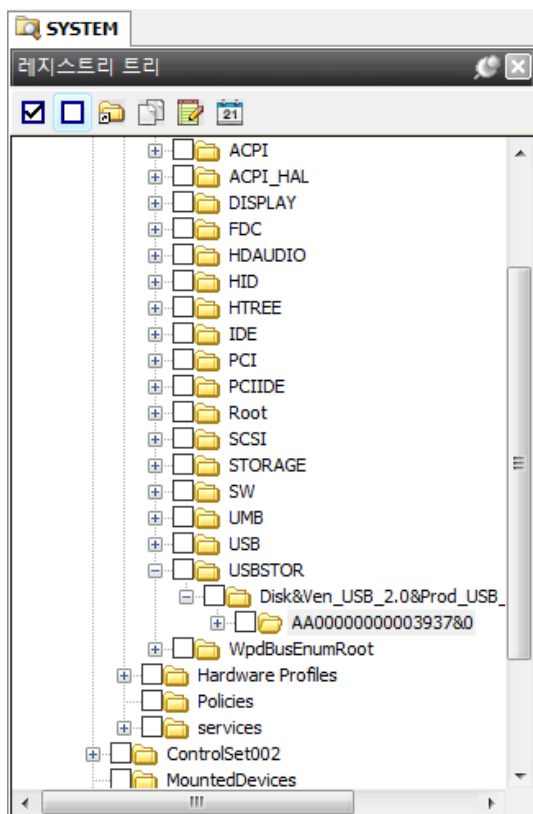
REGA.exe



문제풀이

Device info

HKLM\SYSTEM\ControlSet00\Enum\USBSTOR



값 이름	값 종류	값 데이터
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Capabilities	REG_DWORD	00000010
HardwareID	REG_MULTI_SZ	USBSTOR\DiskUSB_2.0_USB_Flash_Drive_1100 USBSTO...
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW
ContainerID	REG_SZ	{730460c0-2925-5f38-a4f2-8dcf0ec492aa}
ConfigFlags	REG_DWORD	00000000
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\W0001
Class	REG_SZ	DiskDrive
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
Service	REG_SZ	disk
FriendlyName	REG_SZ	USB 2.0 USB Flash Drive USB Device

문제풀이

Serial Number


HKLM\SOFTWARE\Microsoft\WindowsPortableDevices\Devices



문제풀이

Volume Label

HKLM\SOFTWARE\Microsoft\WindowsPortableDevices\Devices

값 이름	값 종류	값 데이터
 FriendlyName	REG_SZ	E:₩₩

문제풀이

Volume Label

HKLM\SYSTEM\ControlSet00\Enum\WpdBusEnumRoot\UMB

값 이름	값 종류	값 데이터
Capabilities	REG_DWORD	000000A4
HardwareID	REG_MULTI_SZ	
CompatibleIDs	REG_MULTI_SZ	wpdbusenum\Wfs
ContainerID	REG_SZ	{730460c0-2925-5f38-a4f2-8dcf0ec492aa}
ConfigFlags	REG_DWORD	00000000
ClassGUID	REG_SZ	{eec5ad98-8080-425f-922a-dabf3de3f69a}
Driver	REG_SZ	{eec5ad98-8080-425f-922a-dabf3de3f69a}\W0000
Class	REG_SZ	WPD
Mfg	REG_SZ	USB 2.0
Service	REG_SZ	WUDFRd
DeviceDesc	REG_SZ	USB Flash Drive
FriendlyName	REG_SZ	E:\

문제풀이

최초 연결 시간

C:\Windows\inf\Setupapi.dev.log

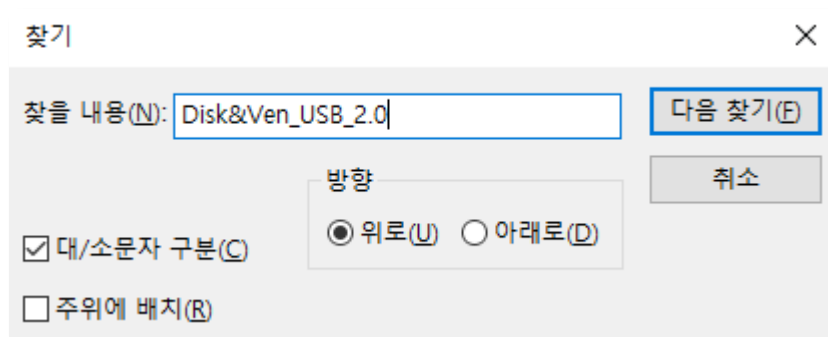
The screenshot displays a forensic analysis tool interface. On the left, the 'Evidence Tree' shows a directory structure with 'Windows' and 'inf' folders highlighted. On the right, the 'File List' pane shows a table of files in the 'C:\Windows\inf' directory. The file 'setupapi.dev.log' is selected, and a context menu is open over it, showing options like 'Export Files...', 'Export File Hash List...', and 'Add to Custom Content Image (AD1)'.

Name	Size	Type	Date Modified
sbp2.PNF.FileSlack	1	File Slack	
sceregvl.inf	15	Regular File	2010-11-21 ...
sceregvl.inf.FileSlack	2	File Slack	
scrapdo.inf	2	Regular File	2009-07-14 ...
scrapdo.inf.FileSlack	3	File Slack	
scrapdo.PNF	5	Regular File	2009-07-14 ...
scrapdo.PNF.FileSlack	4	File Slack	
scsdev.inf	58	Regular File	2009-07-14 ...
scsdev.inf.FileSlack	3	File Slack	
scsdev.PNF	81	Regular File	2009-07-14 ...
scsdev.PNF.FileSlack	4	File Slack	
sdbus.inf	12	Regular File	2010-11-21 ...
sdbus.PNF	19	Regular File	2009-07-14 ...
sdbus.PNF.FileSlack	2	File Slack	
secrecs.inf	9	Regular File	2010-11-21 ...
secrecs.inf.FileSlack	4	File Slack	
sensorsalsdriver.inf	8	Regular File	2010-11-21 ...
setupapi.app.log	19	Regular File	2020-10-09 ...
setupapi.dev.log			2020-10-09 ...
setupapi.ev1			2020-10-09 ...
setupapi.ev2			2020-10-09 ...
setupapi.ev3			2020-10-09 ...

문제풀이

최초 연결 시간

C:\Windows\inf\Setupapi.dev.log



문제풀이

최초 연결 시간

C:\Windows\inf\Setupapi.dev.log

```
>>> [Device Install (Hardware initiated) - USBSTOR\Disk&Ven_USB_2.0&Prod_USB_Flash_Drive&Rev_1100\AA0000000003937&0]
>>> Section start 2020/10/09 13:25:18.943
ump: Creating Install Process: DrvInst.exe 13:25:18.945
ndv: Retrieving device info...
ndv: Setting device parameters...
ndv: Searching Driver Store and Device Path...
dvi: {Build Driver List} 13:25:18.950
dvi: Searching for hardware ID(s):
dvi: usbstor\diskusb_2.0_usb_flash_drive_1100
dvi: usbstor\diskusb_2.0_usb_flash_drive_
dvi: usbstor\diskusb_2.0_
dvi: usbstor\usb_2.0_usb_flash_drive_1
dvi: usb_2.0_usb_flash_drive_1
dvi: usbstor\gendisk
dvi: gendisk
dvi: Searching for compatible ID(s):
```

Forensic

Trace U

600

Trace USB

600

누군가 나의 PC에 악성 프로그램이 담긴 USB를 꽂아 사용한 것 같다.

해당 USB와 관련된 정보를 다 모으자

Flag = scpCTF{시리얼번호_최초연결시간(월_일_시_분)_볼륨 명}

최초연결시간은 24시 표기법을 사용한다.

USB.egg

scpCTF{AA00000000003937_10_09_13_25_E}

Submit

in Army's cipher

700

문제목록

Forensic

Trace USB

600

Crypto

German Army's cipher

700

Forensic

Trace U

600

Challenge

0 Solves



German Army's cipher

700

먼 타국에서 공부를 하고 있는 친구에게 이메일이 왔다.

이게 무슨 말인지....

한번 알아보자.

Flag is upper case letter

GermanArmy's_ci...

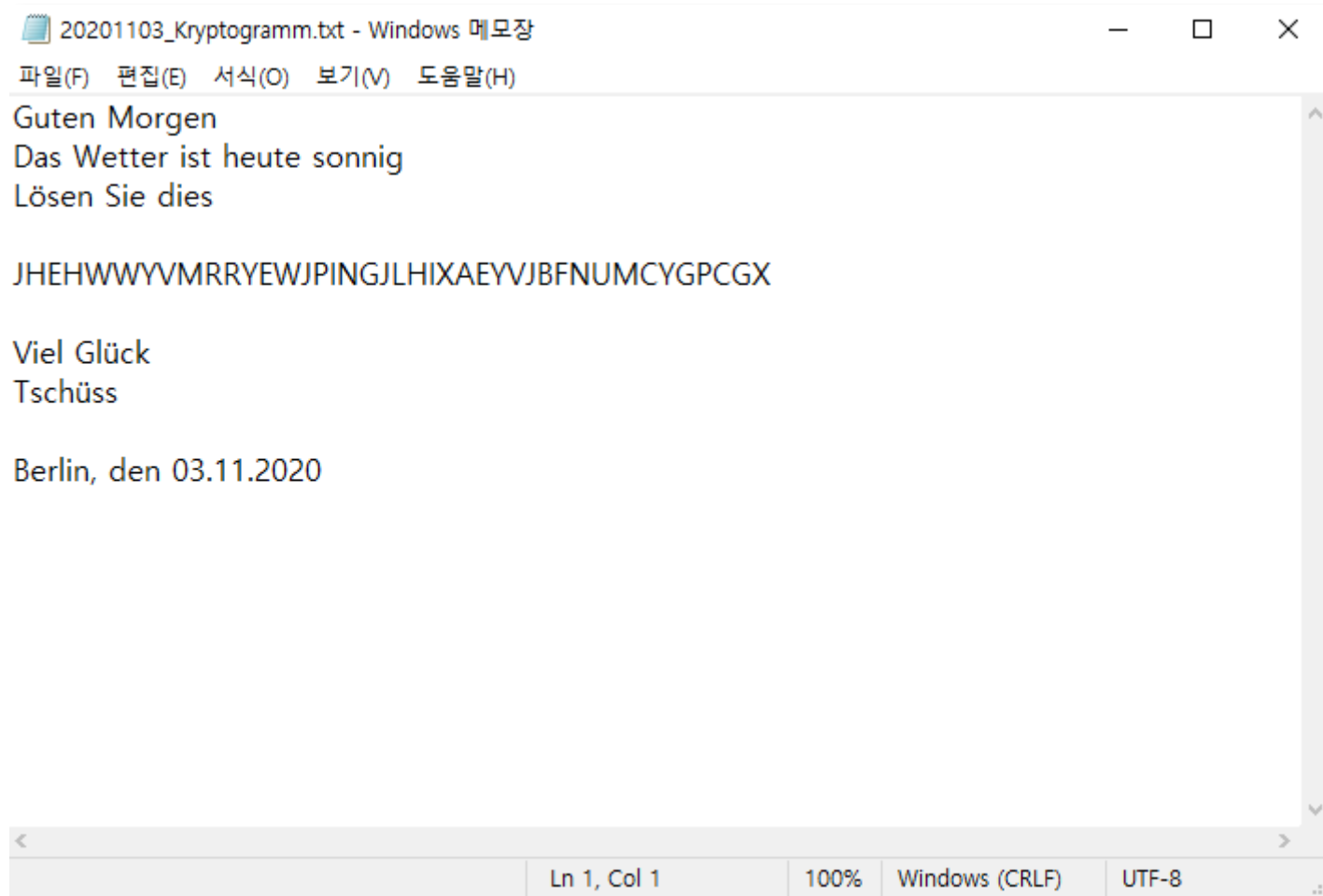
scpCTF{...}

Submit

in Army's cipher

700

문제풀이



문제풀이

독일어 ▼	↔	한국어 ▼
Guten Morgen Das Wetter ist heute sonnig Lösen Sie dies	×	좋은 아침 오늘 날씨는 맑습니다 이것을 해결하십시오
JHEHWWYVMRR YEWJPINGJLHIX AEYVJBFNUMCY GPCGX		JHEHWWYVMRRYEWJPI NGJLHIXAEYVJBFNUMC YGPCGX
Viel Glück Tschüss		행운을 빕니다 안녕
Berlin, den 03.11.2020		베를린, 2020 년 11 월 3 일 joh-eun achim oneul nalssineun malgseubnida igeos-eul haegyeolhasibsio
		JHEHWWYVMRRYEWJPINGJLHIXAEY VJBFNUMCYGPCGX

ENIGMA

문제풀이

ENIGMA



Wehrmacht

Enigma I

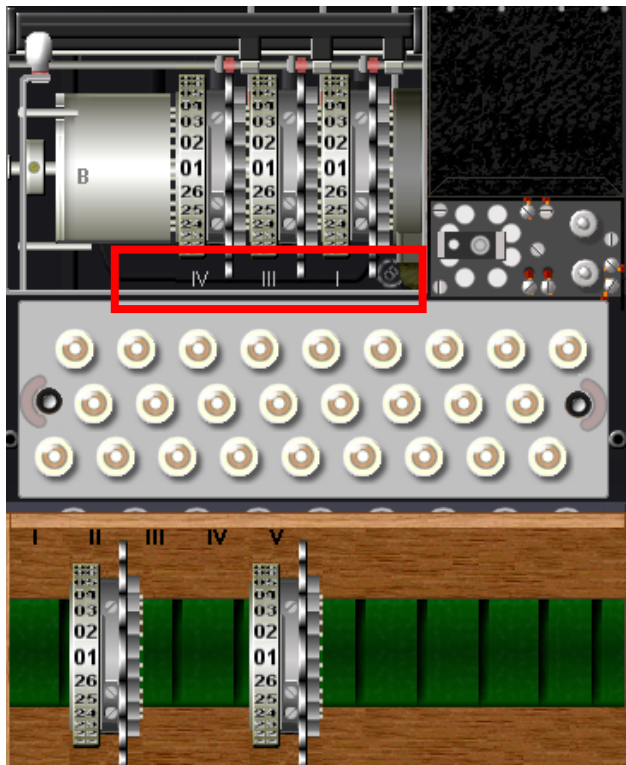
Rotor I, II, III, IV, V

UKW B, UKW C

문제풀이

암호문 만들기

| 03 | **IV III I** | | 13 17 10 | AF BG EK HO JZ LR NX PV SW TU | SLL DIQ WVN NCR |



GEHEIM!

2020_JBUCTF

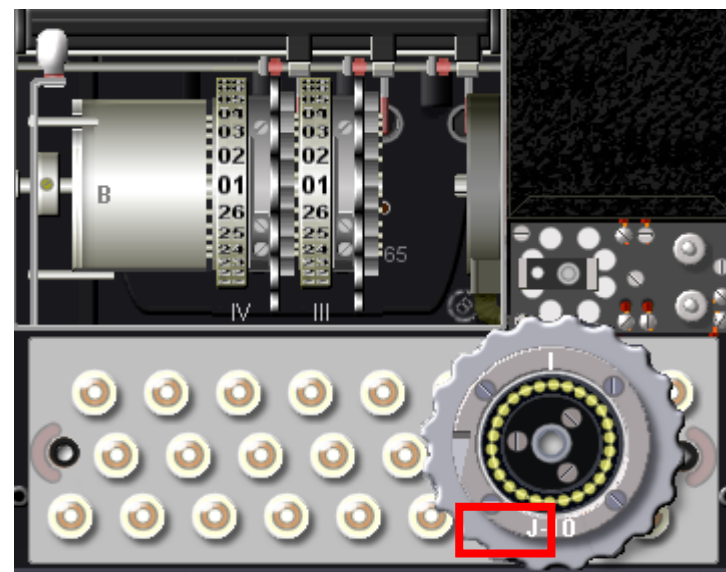
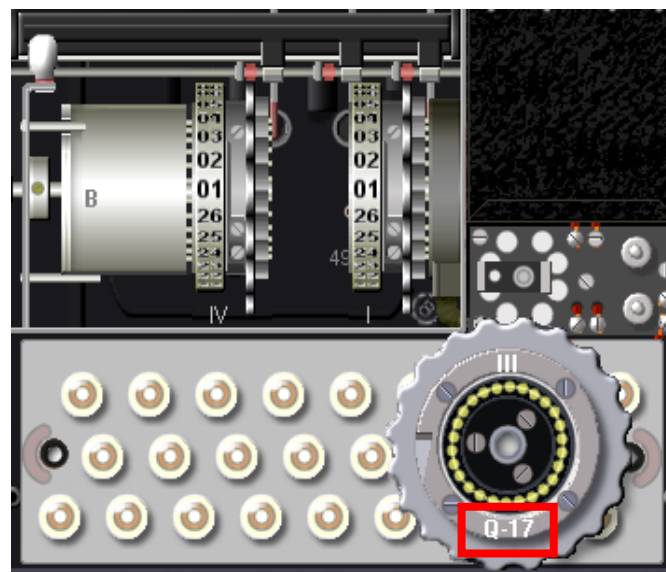
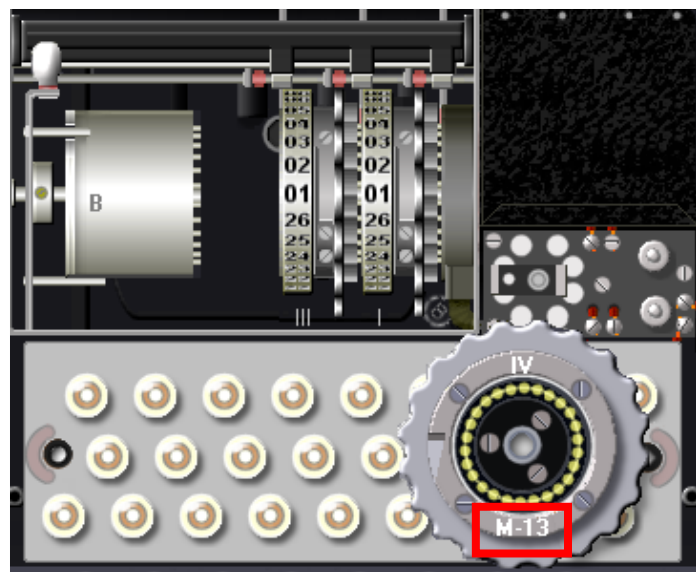
NOVEMBER 2020

Tag	Walzenlage	Ringstellung	Steckerverbindungen	Kennguppen
30	IV V III	14 01 01	AI CF DS EN GQ HM JV LO PZ XY	ZAR IWD JPB ROO
29	V IV I	22 10 09	AU BQ CS DZ EN FW GO JM KX LT	RXU SPS ZKU NSZ
28	V I II	14 19 09	AI CS DQ EY GM HR JL PW TX UV	RQJ DVB VWQ WBO
27	IV I III	15 21 12	BZ CI DO EQ FW GX HL JS NV PR	ZSO AZY NHY WJH
26	IV I II	08 26 03	AK BM CY DT EZ FO GQ JW LN RX	PIN VIX TKD IEH
25	II III I	03 16 04	CR EI HL JY KN MP QT SV UZ WX	NEP NBO TPL STL
24	IV I V	16 02 06	AX BU DT EF GK IN LO PZ QR VY	TRJ QTZ ZTA OJL
23	III V I	19 13 15	AI BL CD EV GM JX NO PU RW SY	ZNF FLH RYC BQI
22	V II IV	11 06 11	AB CV DG ES FY HZ KW LU NO PT	DBQ BYK KNE WVB
21	II IV I	26 16 14	AM DE FI GT HX JR KQ LP OV SU	KJJ TRI BYS VAG
20	III II V	23 11 15	BW CV DI ER FO GY JM KZ LT NP	PQC KCF MCX PIF
19	V I IV	01 06 07	AD BO CX EJ FP GR IT KZ LN MV	COM WJE SFN LXS
18	IV III I	15 19 16	AR BJ CY ET FN HU KX LZ PV QW	QCW IAR KFG LWS
17	II IV I	08 02 23	AJ BN CL DZ EP GM IY OW QR ST	HWL KHL YJD XYQ
16	I IV V	04 02 19	AR CV DM FS GN HL IO KP QW TY	NPL MKM GPR LKI
15	I V II	26 13 07	BP CT DK EQ GH LZ NW OS RY UX	NCN ZWY MTM MZG
14	IV II III	26 15 17	BL CP EV FS GT HM NR OW UX YZ	SYM AGM RDZ MMU
13	V III IV	23 26 04	CF DN ER GX HU IO KZ MV SW TY	FJD XHR SXT GHL
12	III I II	14 14 10	BW CT ER GH IP JY LQ MV OX SZ	UOZ GUH CHS VTW
11	IV I II	16 09 24	AX BP DF EJ GU HV IQ KM OY RT	GON SBS JSA MOT
10	I II III	07 14 01	AF CG DH IU JV KO LT PY QX RW	ZZE GMD DOK YYK
09	II IV III	04 17 25	AE DH FY GS JT LO MQ NP RV UZ	LEY VDA SWF QXP
08	II I III	08 02 18	AU CG DV FQ IO JR KX MY NT SW	XZG WQP FUS BAW
07	V I IV	09 12 20	BD CF EN GT HL IS JZ MX OR PW	NCP OPL ZKJ PPM
06	IV II III	17 22 14	AF CG DN EI HR KU LY MT OV PS	LBR ZON WYD KNE
05	I IV II	21 06 12	AC BQ DH EG FZ IN JM KP LS RW	PQE XXE QNN IIE
04	III II IV	14 14 13	BH DT FL GJ KZ NS OV PY OW UX	DEF LPK ZIJ VGM
03	IV III I	13 17 10	AF BG EK HO JZ LR NX PV SW TU	SLL DIQ WVN NCR
02	III IV II	09 12 23	AJ BR CW EN HV KY LM OS PT QX	QDM PPR OHZ GWK
01	IV V I	05 10 13	CR DL EY HX IP JZ KO MW QS TU	KGM YWD KZY UCE

문제풀이

암호문 만들기

| 03 | IV III I | **13 17 10** | AF BG EK HO JZ LR NX PV SW TU | SLL DIQ WVN NCR |



문제풀이

암호문 만들기

| 03 | IV III I | 13 17 10 | **AF BG EK HO JZ LR NX PV SW TU** SLL DIQ WVN NCR |



문제풀이

암호문 복호화

VIEW

Text ▼

JHEHWWYVMRRYEWJPI NGJLHIXAEYVJB FNUMCYGPCGX

ENCODE DECODE

Enigma machine ▼

MODEL

Enigma I ▼

REFLECTOR

UKW B ▼

ROTOR 1

IV ▼

POSITION

- 1 A +

RING

- 13 M +

ROTOR 2

III ▼

POSITION

- 1 A +

RING

- 17 Q +

ROTOR 3

I ▼

POSITION

- 1 A +

RING

- 10 J +

PLUGBOARD

AF BG EK HO JZ LR NX PV SW TU

VIEW

Text ▼

scpscploxlidvgkhacwbauxhhlaikeqbftqtcrtv

문제풀이

암호문 복호화

VIEW Text ▼	ENCORE DECODE + Enigma machine ▼	VIEW Text ▼																											
VMMRRYEWJPIGJLHIXAEYVJBFCNUMCYGPCGX	<table><tr><td>MODEL</td><td colspan="2">Enigma I ▼</td></tr><tr><td>REFLECTOR</td><td colspan="2">UKW B ▼</td></tr><tr><td>ROTOR 1</td><td>POSITION</td><td>RING</td></tr><tr><td>IV ▼</td><td>- 19 S +</td><td>- 13 M +</td></tr><tr><td>ROTOR 2</td><td>POSITION</td><td>RING</td></tr><tr><td>III ▼</td><td>- 3 C +</td><td>- 17 Q +</td></tr><tr><td>ROTOR 3</td><td>POSITION</td><td>RING</td></tr><tr><td>I ▼</td><td>- 16 P +</td><td>- 10 J +</td></tr><tr><td>PLUGBOARD</td><td colspan="2">AF BG EK HO JZ LR NX PV SW TU</td></tr></table>	MODEL	Enigma I ▼		REFLECTOR	UKW B ▼		ROTOR 1	POSITION	RING	IV ▼	- 19 S +	- 13 M +	ROTOR 2	POSITION	RING	III ▼	- 3 C +	- 17 Q +	ROTOR 3	POSITION	RING	I ▼	- 16 P +	- 10 J +	PLUGBOARD	AF BG EK HO JZ LR NX PV SW TU		enigmacipherisveryfunbutalittlehard
MODEL	Enigma I ▼																												
REFLECTOR	UKW B ▼																												
ROTOR 1	POSITION	RING																											
IV ▼	- 19 S +	- 13 M +																											
ROTOR 2	POSITION	RING																											
III ▼	- 3 C +	- 17 Q +																											
ROTOR 3	POSITION	RING																											
I ▼	- 16 P +	- 10 J +																											
PLUGBOARD	AF BG EK HO JZ LR NX PV SW TU																												

Forensic

Trace U

600

Challenge

0 Solves



German Army's cipher

700

먼 타국에서 공부를 하고 있는 친구에게 이메일이 왔다.

이게 무슨 말인지....

한번 알아보자.

Flag is upper case letter

GermanArmy's_ci...

scpCTF{ENIGMACIPHERISVERYFUNBU.....

Submit

in Army's cipher

700

문제목록

Forensic

Trace USB

600

Crypto

German Army's cipher

700

감사합니다.