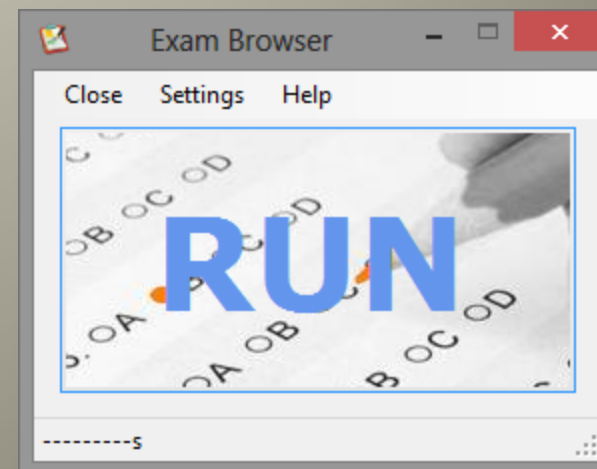
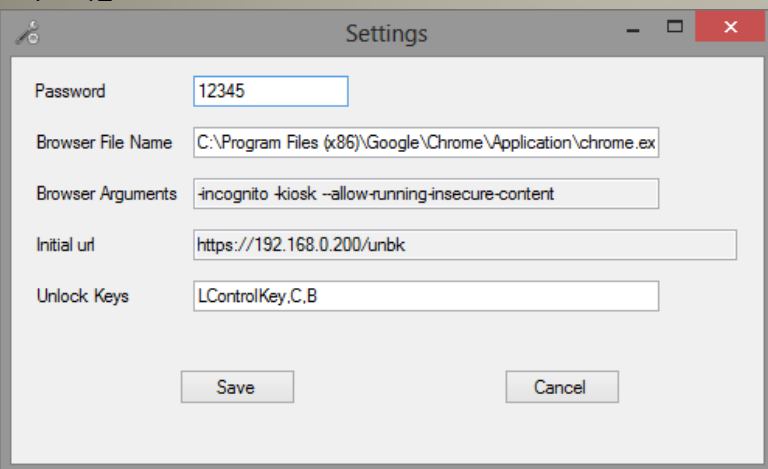












# Analisis Exambro Client

By Lazy\_Cat

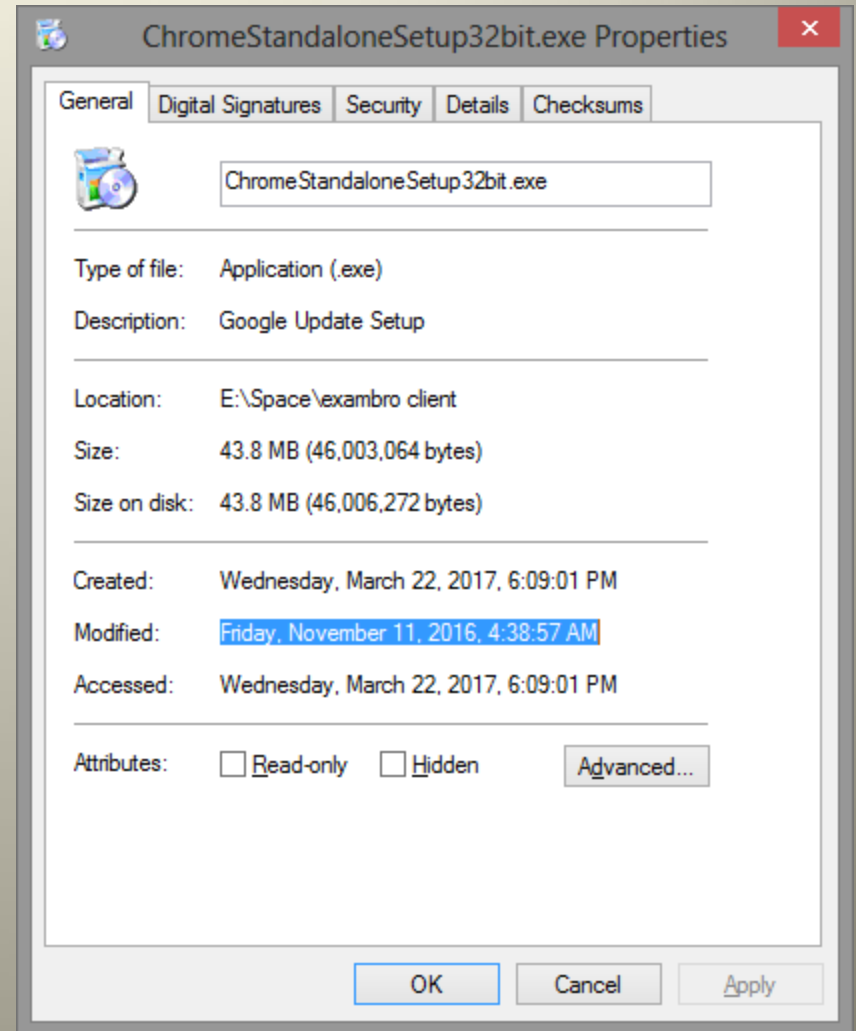
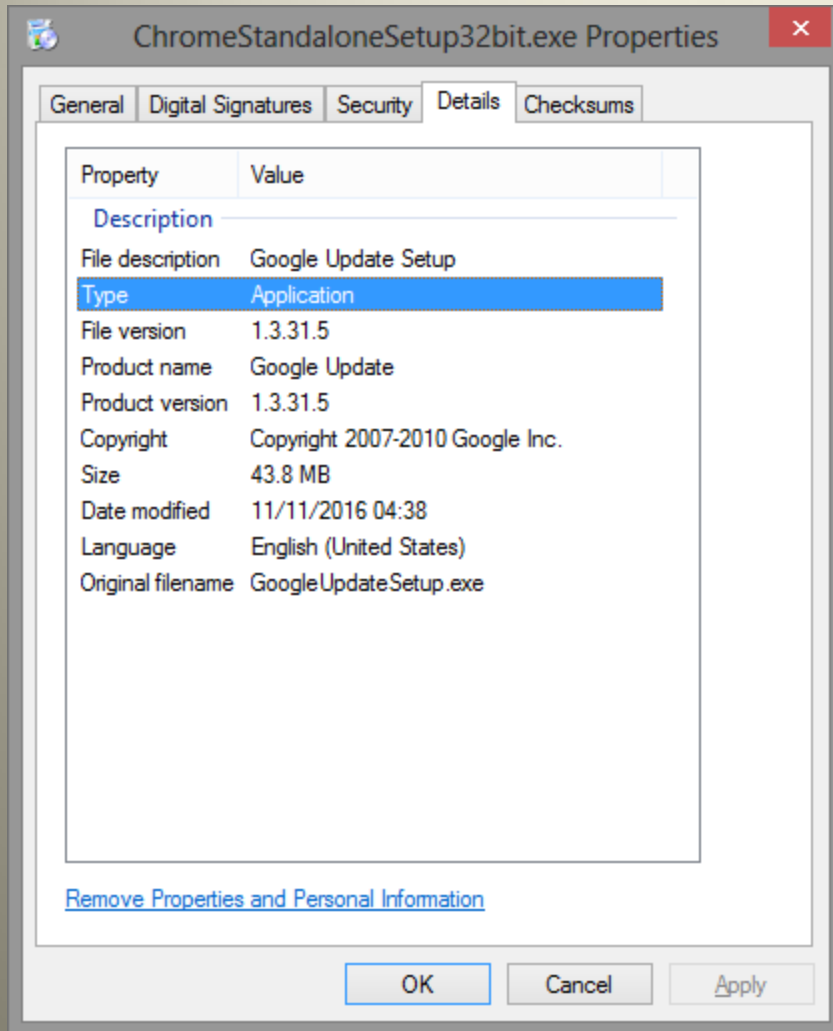


# Exambro Client

Pada client terdapat file-file sbb

	ChromeStandaloneSetup32bit.exe	11/11/2016 04:38	Application	44,925 KB
	ChromeStandaloneSetup64bit.exe	11/11/2016 04:37	Application	49,067 KB
	eb000.dat	3/16/2016 21:25	DAT - MPEG vide...	1 KB
	eb001.dat	3/11/2017 10:10	DAT - MPEG vide...	1 KB
	ExamBrowser.exe	11/5/2016 07:17	Application	991 KB
	ExamBrowser.exe.Config	3/11/2017 10:10	CONFIG File	3 KB
	ExamBrowser.vshost.exe.Config	5/8/2016 15:43	CONFIG File	3 KB
	ExamBrowser.XmlSerializers.dll	1/8/2016 20:04	Application extens...	44 KB
	Gma.UserActivityMonitor.dll	2/6/2015 16:45	Application extens...	28 KB
	log.txt	3/14/2017 11:57	Text Document	4 KB

# Chrome Installer (32bit dan 64bit)



# eb000.dat

The image shows two windows from a Windows operating system. The top window is 'CI Hex Viewer - version 1.3' by SysDev Laboratories. It displays a hex dump of a file named 'eb000.dat'. The address 00000037 is selected. The bottom window is 'eb000.dat - Notepad', which shows the ASCII representation of the selected hex data.

**CI Hex Viewer - version 1.3**

File Edit View Tools

eb001.dat eb000.dat

[HEX] 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ◀ 16 ▶

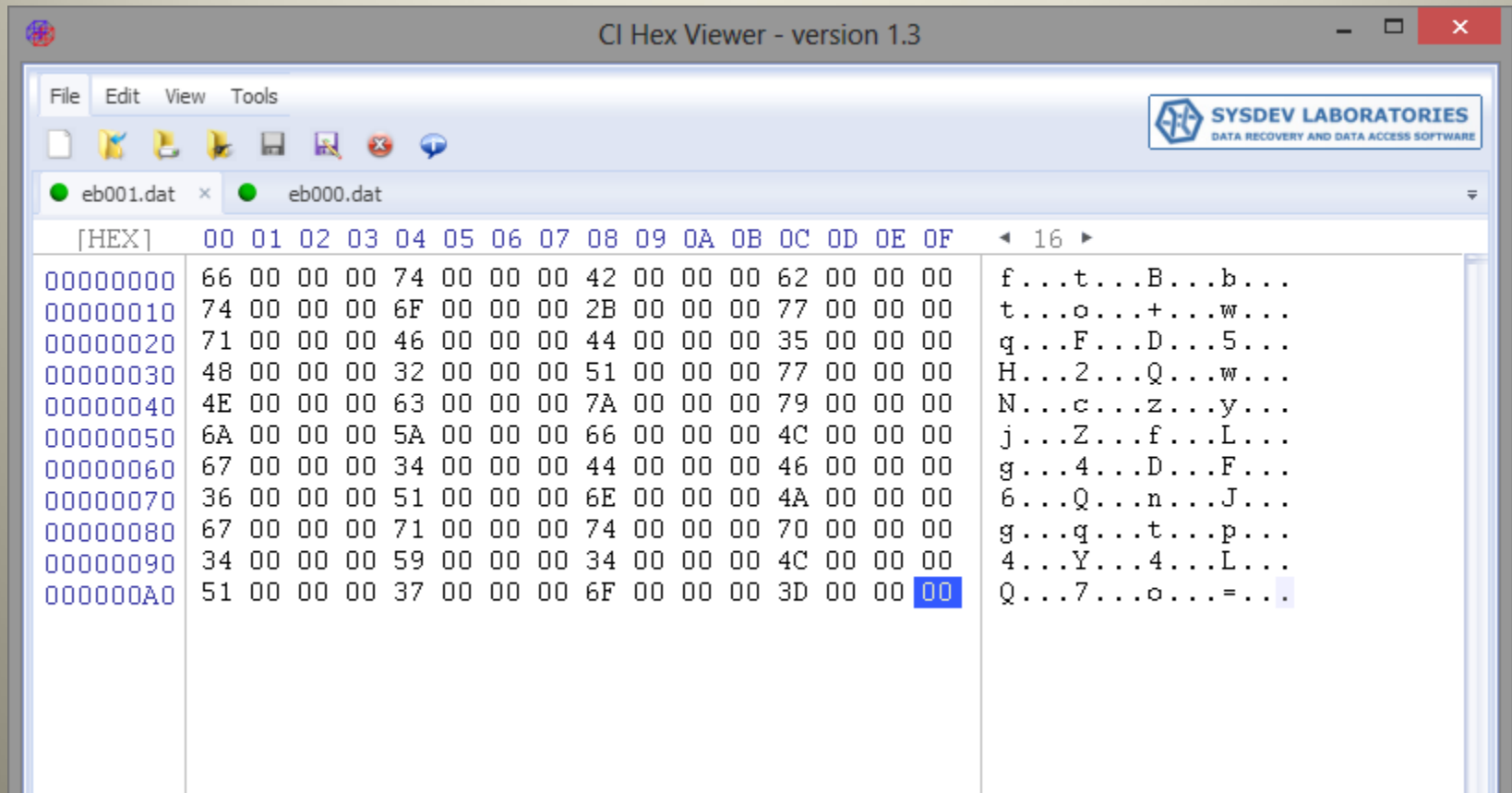
Address	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	ASCII
00000000	37	00	00	00	51	00	00	00	5A	00	00	00	68	00	00	7...Q...Z...h...
00000010	2F	00	00	00	69	00	00	00	66	00	00	00	38	00	00	/...i...f...8...
00000020	77	00	00	00	54	00	00	00	64	00	00	00	67	00	00	w...T...d...g...
00000030	45	00	00	00	42	00	00	00	32	00	00	00	70	00	00	E...B...2...p...
00000040	56	00	00	00	42	00	00	00	70	00	00	00	73	00	00	V...B...p...s...
00000050	6D	00	00	00	51	00	00	00	3D	00	00	00	3D	00	00	m...Q...=...=...

**eb000.dat - Notepad**

File Edit Format View Help

7 Q Z h / i f 8 w T d g E B 2 p V B p s m Q = =

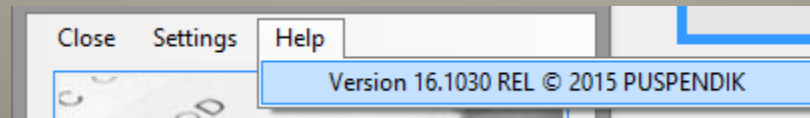
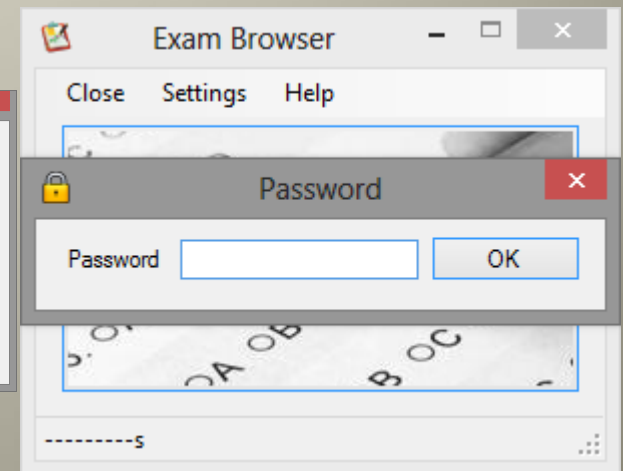
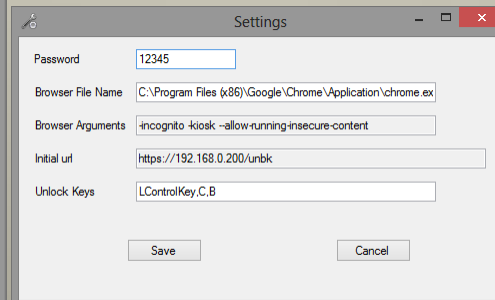
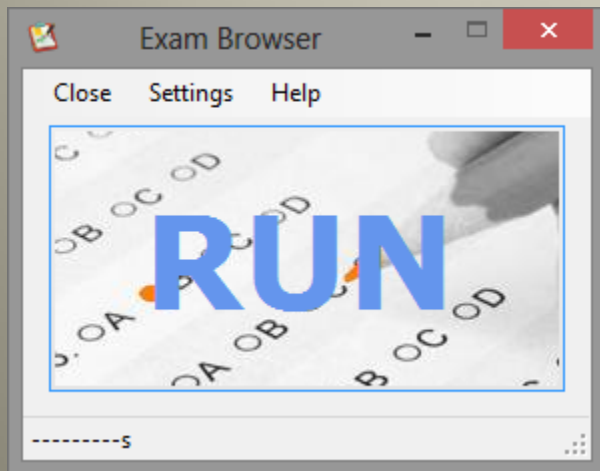
# eb001.dat



# ExamBrowser.exe

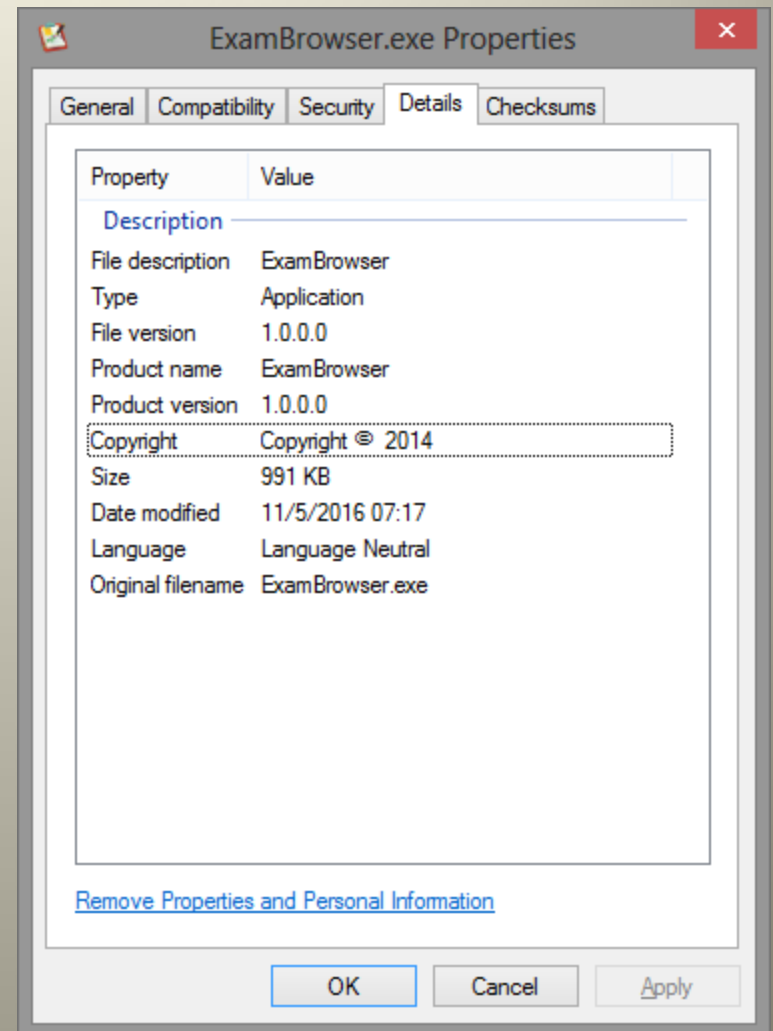
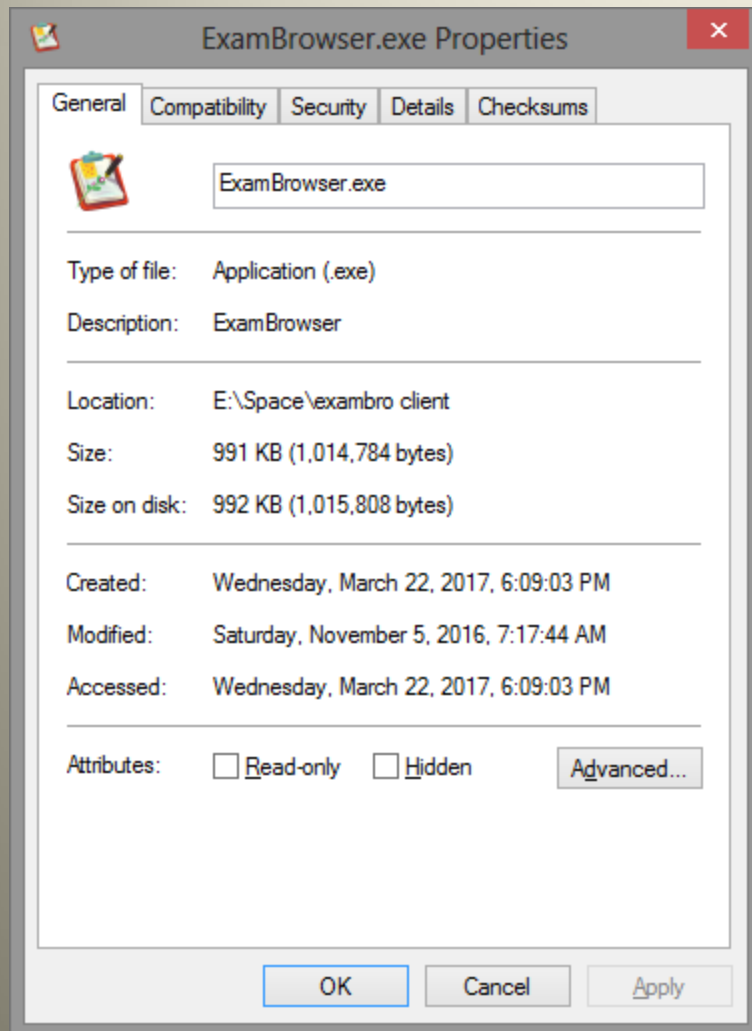
Terdapat empat fungsi yaitu

- Close : fungsinya ya untuk menutup program
- Settings : minta password untuk membuka (tentu kita dapat menjebol pw nya haha)
- Help : Version 16.1030 blabla
- RUN : untuk memulai ujian



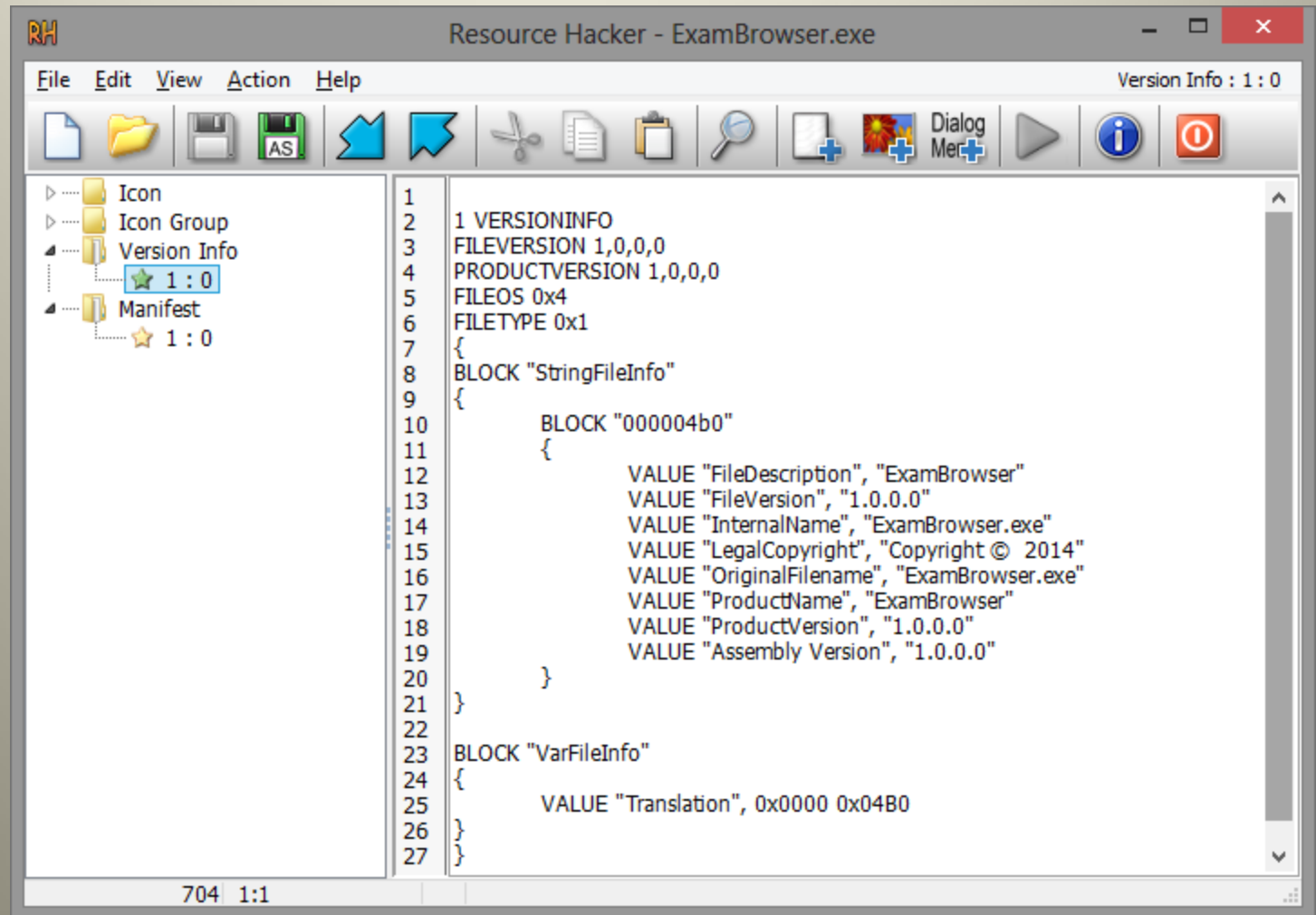
# ExamBrowser.exe

- Properties



# ExamBrowser.exe

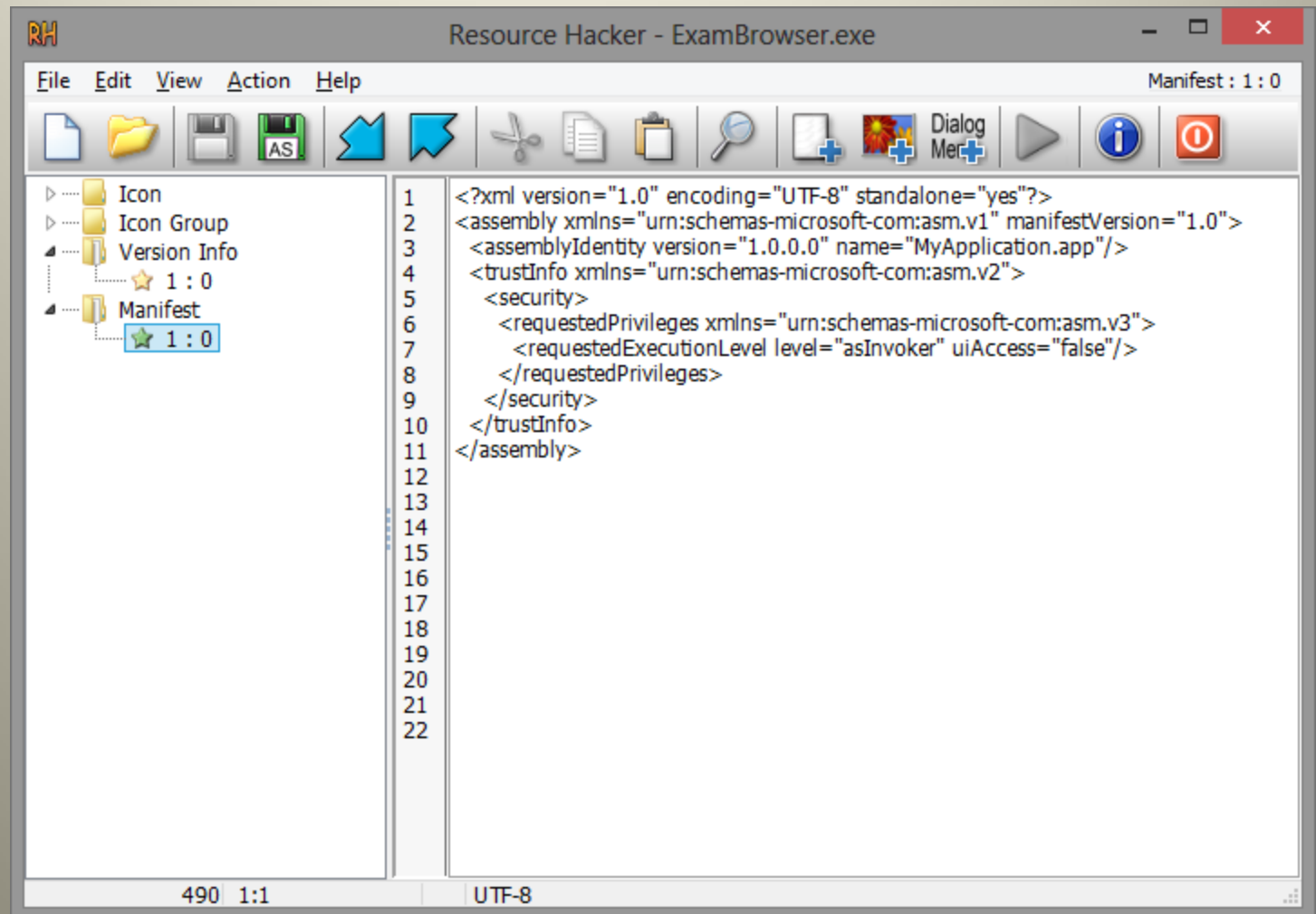
- Version info





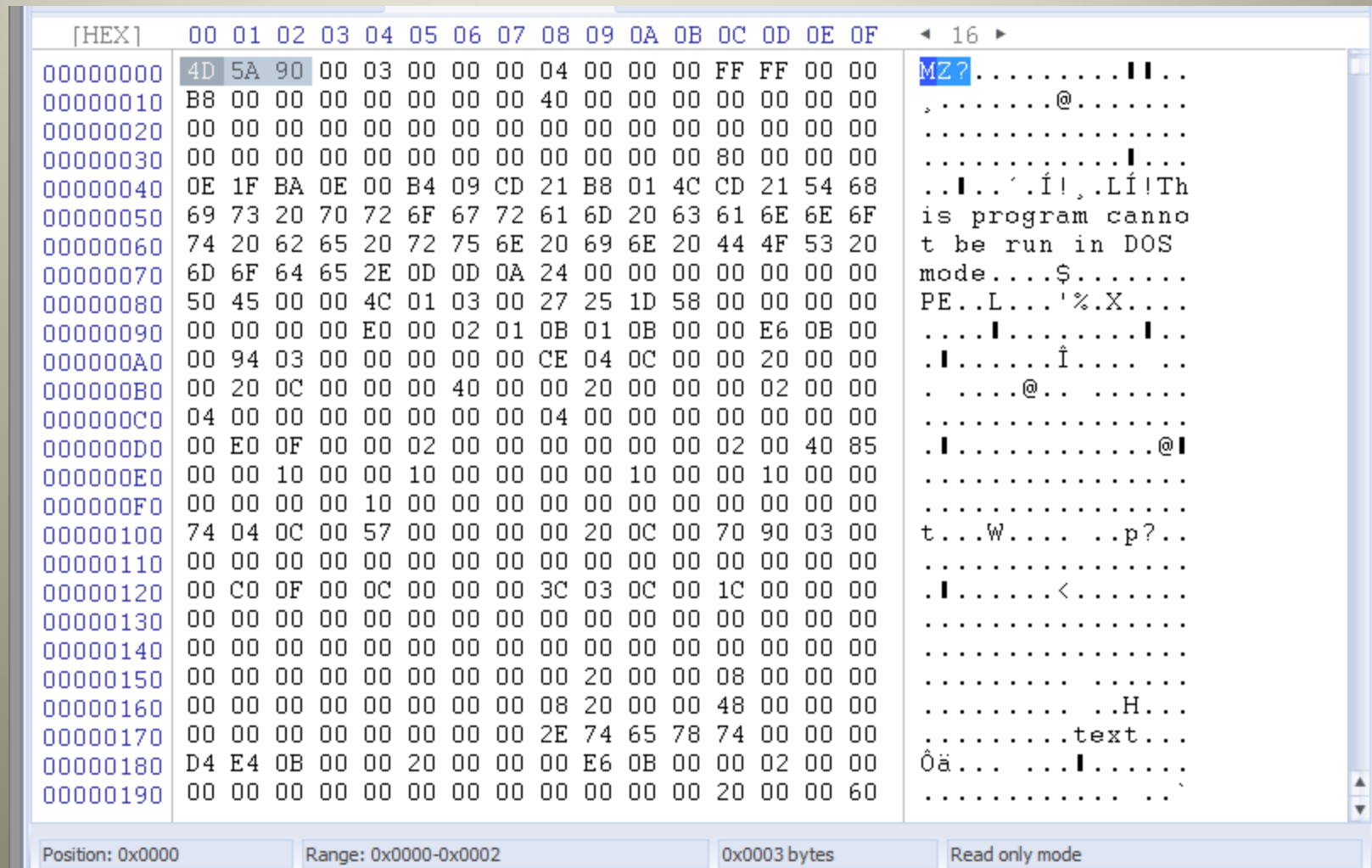
# ExamBrowser.exe

- Manifest



# ExamBrowser.exe

- File Header



```

<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <sectionGroup name="applicationSettings" type="System.Configuration.ApplicationSettingsGroup, System, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >
      <section name="ExamBrowser.Properties.Settings" type="System.Configuration.ClientSettingsSection, System, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"
requirePermission="false" />
    </sectionGroup>
  </configSections>
  <appSettings>
    <add key="Password" value="12345" />
    <add key="BrowserFilename" value="C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" />
    <add key="BrowserArguments" value="-incognito -kiosk --allow-running-insecure-content" />
    <add key="InitialUrl" value="" />
    <add key="Modification Date" value="15:05:52" />
    <add key="TimerInterval" value="0" />
    <add key="HeartInterval" value="60000" />
    <add key="LockKeys" value="0" />
    <add key="DebugMode" value="0" />
    <add key="SpecialKeys" value="LControlKey,C,B" />
    <add key="Keys" value="" />
    <add key="Application" value="" />
    <add key="SendF11Stroke" value="0" />
    <add key="Heslo" value="0" />
    <add key="ClientSettingsProvider.ServiceUri" value="" />
  </appSettings>
  <startup>

<supportedRuntime version="v2.0.50727"/></startup>
  <system.web>
    <membership defaultProvider="ClientAuthenticationMembershipProvider">
      <providers>
        <add name="ClientAuthenticationMembershipProvider" type="System.Web.ClientServices.Providers.ClientFormsAuthenticationMembershipProvider, System.Web.Extensions, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35" serviceUri="" />
      </providers>
    </membership>
    <roleManager defaultProvider="ClientRoleProvider" enabled="true">
      <providers>
        <add name="ClientRoleProvider" type="System.Web.ClientServices.Providers.ClientRoleProvider, System.Web.Extensions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"
serviceUri="" cacheTimeout="86400"/>
      </providers>
    </roleManager>
  </system.web>
  <applicationSettings>
    <ExamBrowser.Properties.Settings>
      <setting name="ExamBrowser_Arthur_WorkstationService_WorkstationService"
serializeAs="String">
        <value>https://192.168.0.200/puspendikunbkservice/CBTservices/WorkstationService.svc</value>
      </setting>
    </ExamBrowser.Properties.Settings>
  </applicationSettings>
</configuration>

```

# ExamBrowser.exe.Config

**\*it's plaintext you can copy and zoom it**

yang biru adalah password exambro

(tak semua password sama)

yang merah adalah hotkey eambro

yang oranye adalah browser argument

yang hijau adalah ip server

```

<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <sectionGroup name="applicationSettings" type="System.Configuration.ApplicationSettingsGroup, System, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >
      <section name="ExamBrowser.Properties.Settings" type="System.Configuration.ClientSettingsSection, System, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"
requirePermission="false" />
    </sectionGroup>
  </configSections>
  <appSettings>
    <add key="Password" value="12345"/>
    <add key="BrowserFilename" value="C:\Program Files\Google\Chrome\Application\chrome.exe"/>
    <add key="BrowserArguments" value="-incognito"/>
    <add key="InitialUrl" value=""/>
    <add key="Modification Date" value=""/>
    <add key="TimerInterval" value="0"/>
    <add key="HeartInterval" value="60000"/>
    <add key="LockKeys" value="0"/>
    <add key="DebugMode" value="0"/>
    <add key="SpecialKeys" value="LControlKey,H,C,B"/>
    <add key="Keys" value=""/>
    <add key="Application" value=""/>
    <add key="SendF11Stroke" value="0"/>
    <add key="Heslo" value=""/>
    <add key="ClientSettingsProvider.ServiceUri" value=""/>
  </appSettings>
  <startup>

<supportedRuntime version="v2.0.50727"/></startup>
  <system.web>
    <membership defaultProvider="ClientAuthenticationMembershipProvider">
      <providers>
        <add name="ClientAuthenticationMembershipProvider" type="System.Web.ClientServices.Providers.ClientFormsAuthenticationMembershipProvider, System.Web.Extensions, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35" serviceUri=""/>
      </providers>
    </membership>
    <roleManager defaultProvider="ClientRoleProvider" enabled="true">
      <providers>
        <add name="ClientRoleProvider" type="System.Web.ClientServices.Providers.ClientRoleProvider, System.Web.Extensions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"
serviceUri="" cacheTimeout="86400"/>
      </providers>
    </roleManager>
  </system.web>
  <applicationSettings>
    <ExamBrowser.Properties.Settings>
      <setting name="ExamBrowser_Arthur_WorkstationService_WorkstationService"
serializeAs="String">
        <value>http://192.168.0.200/puspendikunbkservice/CBTservices/WorkstationService.svc</value>
      </setting>
    </ExamBrowser.Properties.Settings>
  </applicationSettings>
</configuration>

```

# ExamBrowser.vshost.exe.Config

**\*it's plaintext you can copy and zoom it**

**ini adalah default settings exambro!**

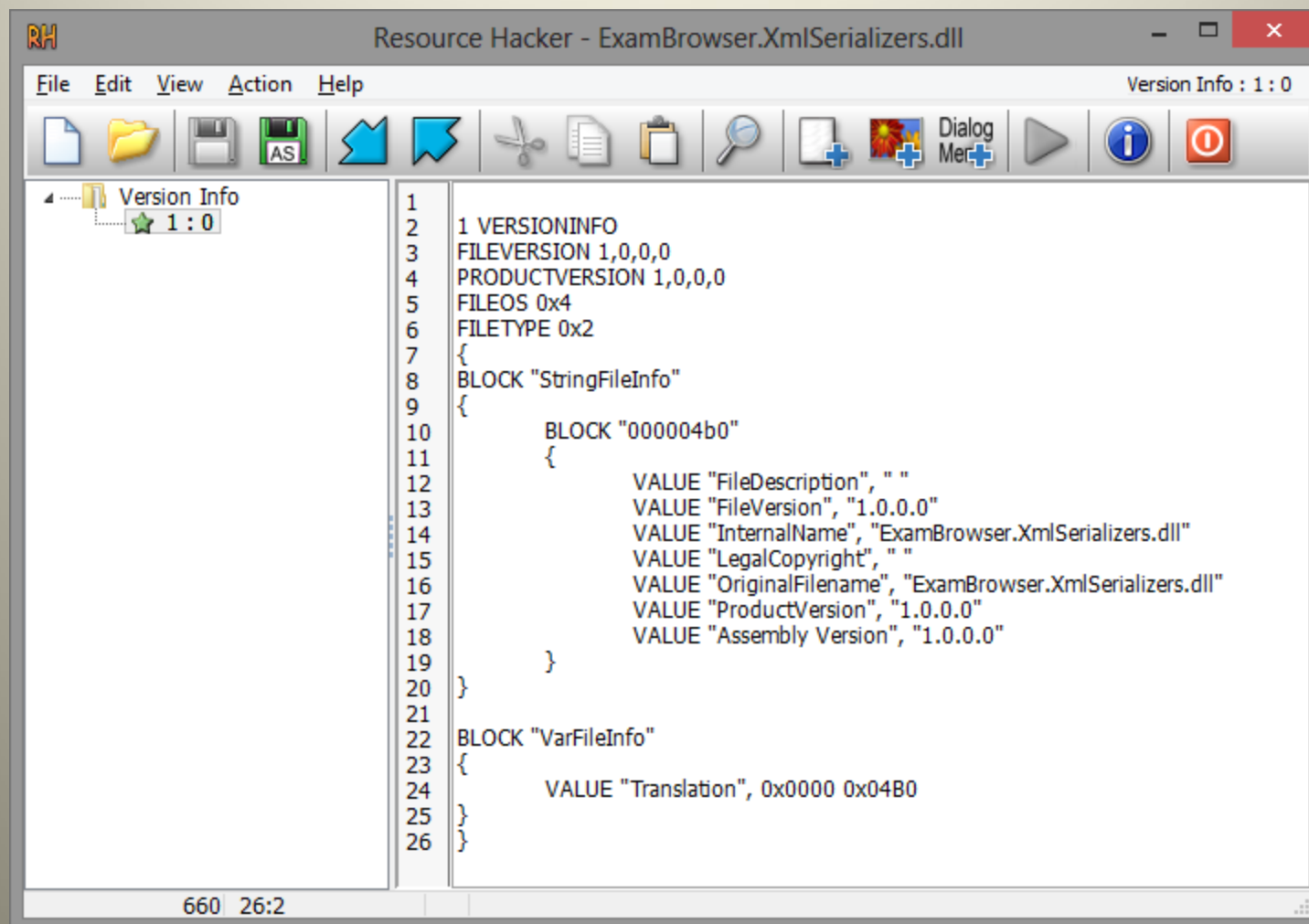
**yang biru adalah password default 12345**

**yang merah adalah hotkey Ctrl+H/C/B**

**yang oranye adalah browser arguments**

**yang hijau adalah ip server**

# ExamBrowser.XmlSerializers.dll

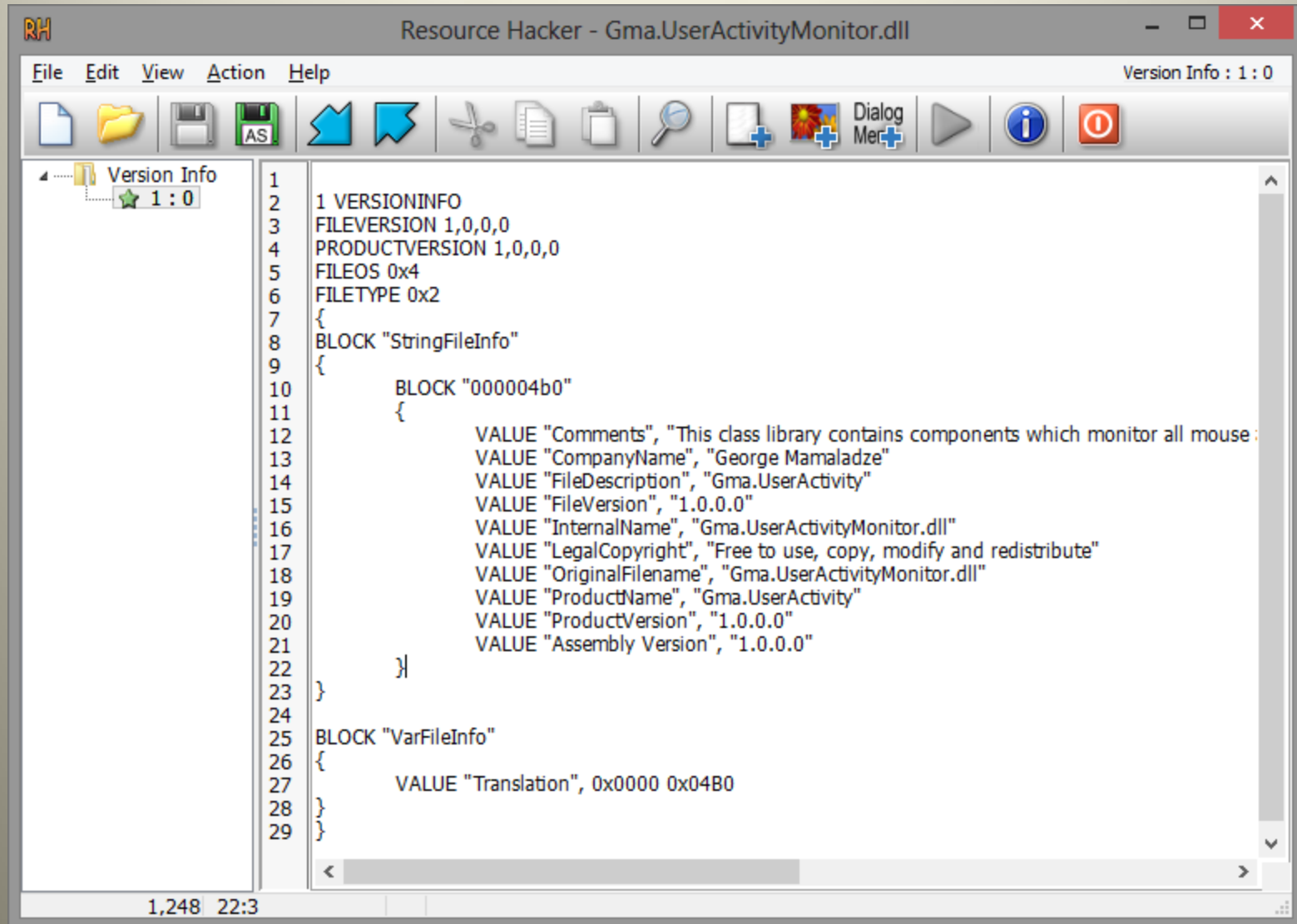


# ExamBrowser.XmlSerializers.dll

[HEX]	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ?.....!!..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	,.....@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	00	.....!...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..!..'í!..Lí!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$.....
00000080	50	45	00	00	4C	01	03	00	C2	B3	8F	56	00	00	00	00	PE..L...Â!IV....
00000090	00	00	00	00	E0	00	02	21	0B	01	08	00	00	80	00	00	....!..!.....!
000000A0	00	20	00	00	00	00	00	00	CE	9F	00	00	00	20	00	00	. ....î!....
000000B0	00	A0	00	00	00	00	40	00	00	20	00	00	00	10	00	00	. ....@..
000000C0	04	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	.....
000000D0	00	E0	00	00	00	10	00	00	00	00	00	00	03	00	40	85	.!.....@!
000000E0	00	00	10	00	00	10	00	00	00	00	10	00	00	10	00	00	.....
000000F0	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00	.....
00000100	78	9F	00	00	53	00	00	00	00	A0	00	00	F0	02	00	00	x!..S.... ..!
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000120	00	C0	00	00	0C	00	00	00	00	00	00	00	00	00	00	00	.!.....
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000150	00	00	00	00	00	00	00	00	00	20	00	00	08	00	00	00	.....
00000160	00	00	00	00	00	00	00	00	08	20	00	00	48	00	00	00	..... ..H...
00000170	00	00	00	00	00	00	00	00	2E	74	65	78	74	00	00	00	.....text...
00000180	D4	7F	00	00	00	20	00	00	00	80	00	00	00	10	00	00	Ô!... ..!
00000190	00	00	00	00	00	00	00	00	00	00	00	00	20	00	00	60	.....

Position: 0xAFFD    [n/a]    [n/a]    Read only mode

# Gma.UserActivityMonitor.dll



# Gma.UserActivityMonitor.dll

VALUE "Comments", "This class library contains components which monitor all mouse and keyboard activities globally (also outside of the application) and provides appropriate events."

VALUE "CompanyName", "George Mamaladze"

VALUE "FileDescription", "Gma.UserActivity"

VALUE "FileVersion", "1.0.0.0"

VALUE "InternalName", "Gma.UserActivityMonitor.dll"

VALUE "LegalCopyright", "Free to use, copy, modify and redistribute"

VALUE "OriginalFilename", "Gma.UserActivityMonitor.dll"

VALUE "ProductName", "Gma.UserActivity"

VALUE "ProductVersion", "1.0.0.0"

VALUE "Assembly Version", "1.0.0.0"



# Gma.UserActivityMonitor.dll

[HEX]	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	◀ 16 ▶
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ?.....  ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	,.....@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	00	.....!...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..!..'í!..Lí!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$......
00000080	50	45	00	00	4C	01	03	00	4E	8D	D4	54	00	00	00	00	PE..L...N!ÔT....
00000090	00	00	00	00	E0	00	02	21	0B	01	0B	00	00	40	00	00	....!...!.....@..
000000A0	00	20	00	00	00	00	00	00	BE	5C	00	00	00	20	00	00	.....!\\... ..
000000B0	00	60	00	00	00	00	00	11	00	20	00	00	00	10	00	00	.. ..
000000C0	04	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	.....
000000D0	00	A0	00	00	00	10	00	00	00	00	00	00	03	00	40	85	.....@!
000000E0	00	00	10	00	00	10	00	00	00	00	10	00	00	10	00	00	.....
000000F0	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00	.....
00000100	6C	5C	00	00	4F	00	00	00	00	60	00	00	38	05	00	00	l\\..0.....8...
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000120	00	80	00	00	0C	00	00	00	00	00	00	00	00	00	00	00	..!.....
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000150	00	00	00	00	00	00	00	00	00	20	00	00	08	00	00	00	.....
00000160	00	00	00	00	00	00	00	00	08	20	00	00	48	00	00	00	..... ..H...
00000170	00	00	00	00	00	00	00	00	2E	74	65	78	74	00	00	00	.....text...
00000180	C4	3C	00	00	00	20	00	00	00	40	00	00	00	10	00	00	Ä<... ..@.....
00000190	00	00	00	00	00	00	00	00	00	00	00	00	20	00	00	60	.....

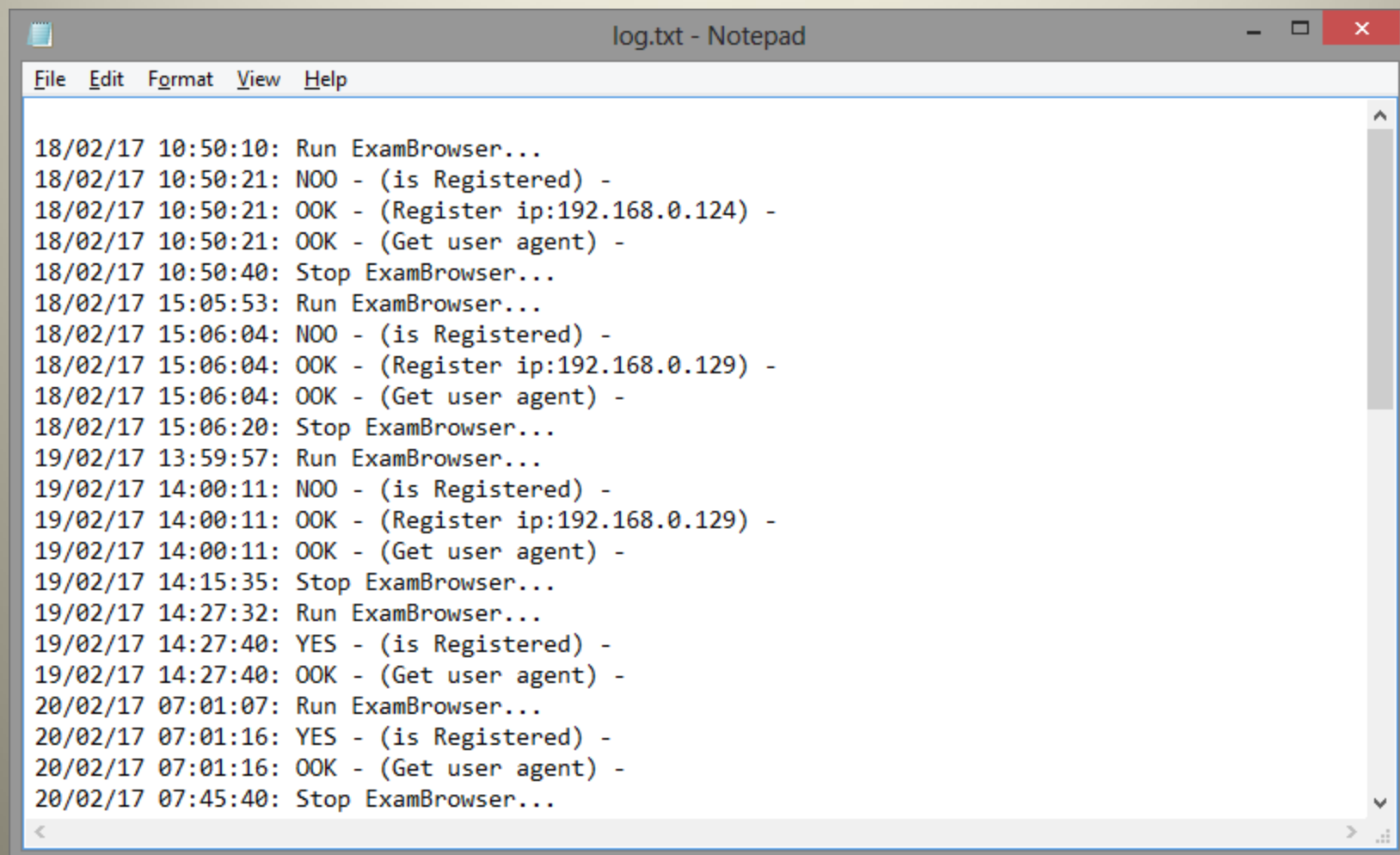
Position: 0x0050

[n/a]

[n/a]

Read only mode

# log.txt



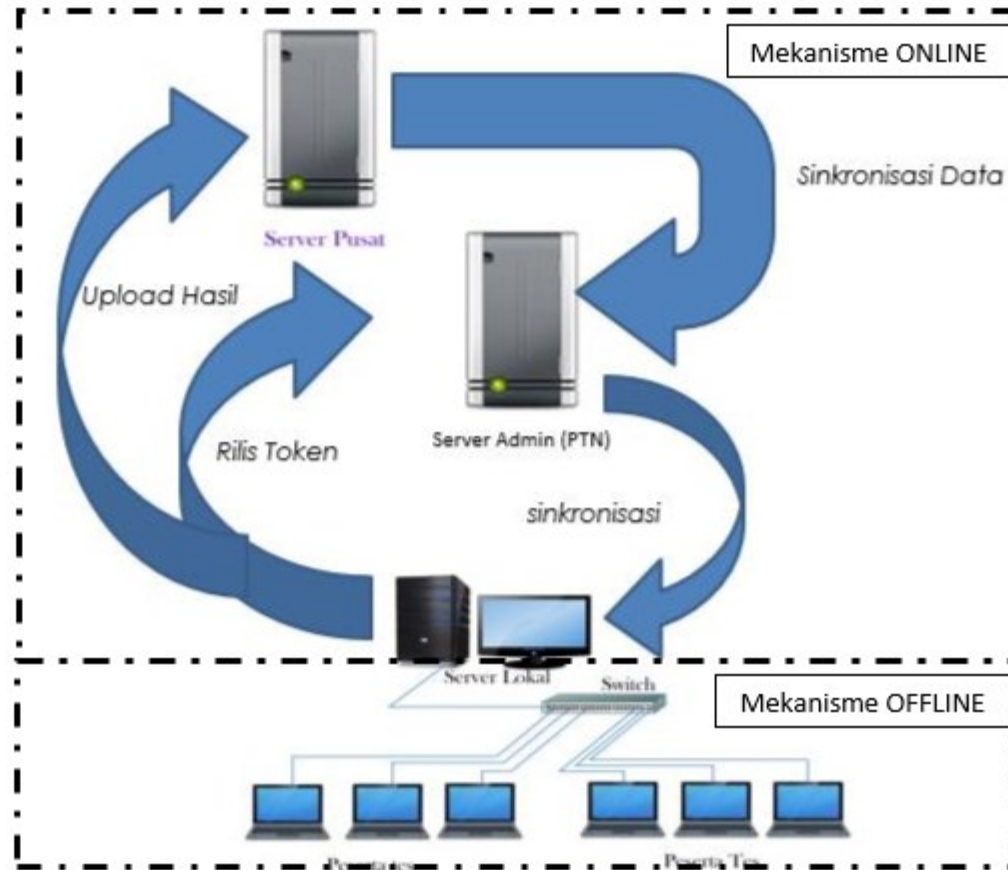
```
log.txt - Notepad
File Edit Format View Help
18/02/17 10:50:10: Run ExamBrowser...
18/02/17 10:50:21: NOO - (is Registered) -
18/02/17 10:50:21: OOK - (Register ip:192.168.0.124) -
18/02/17 10:50:21: OOK - (Get user agent) -
18/02/17 10:50:40: Stop ExamBrowser...
18/02/17 15:05:53: Run ExamBrowser...
18/02/17 15:06:04: NOO - (is Registered) -
18/02/17 15:06:04: OOK - (Register ip:192.168.0.129) -
18/02/17 15:06:04: OOK - (Get user agent) -
18/02/17 15:06:20: Stop ExamBrowser...
19/02/17 13:59:57: Run ExamBrowser...
19/02/17 14:00:11: NOO - (is Registered) -
19/02/17 14:00:11: OOK - (Register ip:192.168.0.129) -
19/02/17 14:00:11: OOK - (Get user agent) -
19/02/17 14:15:35: Stop ExamBrowser...
19/02/17 14:27:32: Run ExamBrowser...
19/02/17 14:27:40: YES - (is Registered) -
19/02/17 14:27:40: OOK - (Get user agent) -
20/02/17 07:01:07: Run ExamBrowser...
20/02/17 07:01:16: YES - (is Registered) -
20/02/17 07:01:16: OOK - (Get user agent) -
20/02/17 07:45:40: Stop ExamBrowser...
```

# PEMBAHASAN

# Cara kerja CBT (semi offline)

UNBK 2017

Gambar berikut ialah ilustrasi UN menggunakan model CBT *semi online*:



Gambar 1 Model UNBK 2017.

## C. Sarana dan Prasarana

Sarana dan prasarana yang dibutuhkan UNBK ialah sebagai berikut:

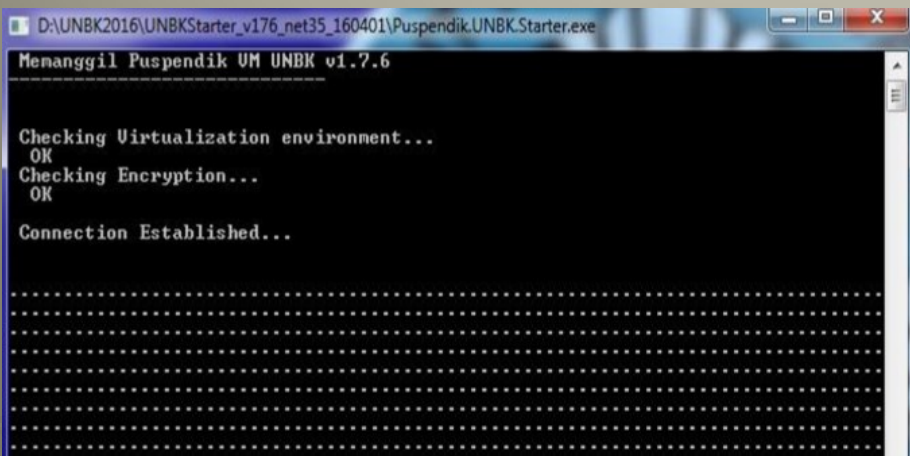
- Satu server lokal, yang akan diakses oleh maksimal 40 komputer peserta.
- Meja komputer memiliki panjang minimal 1 M.
- Jumlah komputer peserta tergantung jumlah server lokal.

Spesifikasi *hardware* minimal server lokal yang harus disediakan untuk UNBK adalah sebagai berikut:

OS : 64 bit dengan Windows 7 / Windows server 8 / Linux.

Prosesor : 4 core dengan frekuensi 1.6 GHz

Server sekolah menggunakan Oracle VM Virtualbox dan Windows Server 2012 R2 dengan ip 192.168.1.200 jadi anda dapat mengexploit server sekolah dengan linux hehe. Tentu anda **harus membuat backdoor** (entah virtual wifi /hardware khusus /evil twin) pada pc atau server atau bahkan router. Karena jaringan terhubung dengan kabel LAN. Dan walaupun demikian server sekolah ada enkripsinya lho

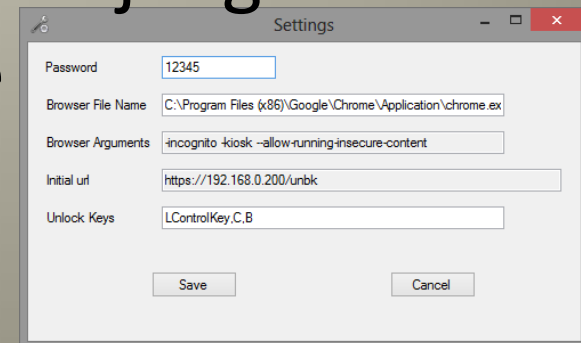


Berdasarkan diagram sebelumnya, tertera bahwa pc yang digunakan user tak terhubung langsung dengan server dinas. Melainkan terhubung dengan server sekolah yang telah disinkronkan (mendapat soal, token, dll) menggunakan CBTSync dengan server dinas dan **waktu sinkron tsb adalah beberapa menit/jam sebelum mulai ujian**. Jadi walau anda bisa menjebol server sekolah, anda tak akan mendapat manfaat apapun. karena soal hanya didapat sesaat sebelum ujian dimulai. Dan walaupun anda dapat memanipulasi database dan mencontek jawaban dengan teman anda yang rank 1 sekalipun, nilai anda bisa saja **JEBLOK**. Karena tak ada jaminan soal anda sama.

Pada awal membuka exambro akan nampak 4 fungsi yaitu close, settings, help dan run.



Seperti yang telah saya jelaskan sebelumnya jika anda ingin membuka setting maka perlu password. Untuk menemukan password tsb cukup membuka folder exambro dan cari *ExamBrowser.exe.Config* dan buka dengan notepad. Jika telah terbuka cari *<add key="Password"* dan ingat password tsb **TANPA TANDA KUTIP**. Password default adalah 12345 dan jika anda telah masuk jangan rubah apapun. Ngko error sukur kwe



Saat user menekan RUN maka akan menjalankan browser Chrome yang dijalankan dengan argument *-incognito -kiosk --allow-running-insecure-content* seperti yang terlihat pada *ExamBrowser.exe.Config*

**-incognito** : adalah mode dimana chrome tak akan mencatat apapun yang user lakukan. Spt history, download, dll

**-kiosk** : adalah mode fullscreen yang membatasi user agar tak mengubah2 tab pada google chrome. Yo mesti moso unbk sisan browsing malah seneng kwe.

**--allow-running-insecure-content** : adalah mode untuk mengijinkan file yang terikat HTTP agar dapat dibuka dalam mode HTTPS. Iki ga penting intine ben ga error wes ngono tok.



Seperti yang telah saya jelaskan sebelumnya bahwa exambro menjalankan chrome dengan argument –kiosk yang berarti user tak bisa berpindah tab dan menekan tombol perintah apapun kecuali ctrl+c+b atau ctrl+h+c+b dan diperparah dengan adanya library Gma.UserActivityMonitor.dll yang berguna untuk *“This class library contains components which monitor all mouse and keyboard activities globally (also outside of the application) and provides appropriate events”* ahmbuh intine Gma.UserActivityMonitor.dll berguna untuk **memonitor segala aktivitas user** seperti keyboard yang ditekan, dan gerak gerik mouse. Lahis kwe

Cara yang paling mungkin namun beresiko adalah keluar dari app exambro **Sebelum anda login** lalu memanipulasi ***ExamBrowser.exe.Config*** dengan notepad. Pada argumen hapus ***-kiosk*** lalu jalankan exambro. Dan browser anda kembali menjadi chrome yang anda kenal. Anda pun dapat membuat LAN chat group. Bahkan hanya dengan menggunakan network sharing bawaan windows. Anda membuat folder dan namai folder tsb dengan pesan anda. Cara ini telah saya gunakan selama tryout dan hampir selalu berhasil. Namun kerugian cara ini adalah segala aktivitas anda dimonitor!!

\*Jika perlu hapus library ***Gma.UserActivityMonitor.dll*** dan jalankan exambro. Menghapus gma.user tak saya rekomendasikan karena dapat membuat exambro menjadi crash.

Cara lain adalah dengan menggunakan keyboard yang terdapat media key. Seperti contoh



Jika anda menekan tombol tsb maka akan muncul Windows Media player dan exambro akan terminimize. Mantab kan setelah itu buat LAN chat dan done... cara paling mudah, senyap, efektif, hampir tak meninggalkan jejak

Segala cara diatas memiliki kekurangan. Yaitu aktivitas anda dimonitor oleh *Gma.UserActivityMonitor.dll*

Dan cara satu-satunya untuk mengelabui gma.user adalah dengan menonaktifkan library tsb. Dengan cara ubah nama atau hapus file tsb. Namun hal ini juga beresiko karena bisa saja menyebabkan exambro crash.

**ATAU anda dapat menjebol server dinas langsung. Dan mendownload soal2 dari server tsb bahkan merubah nilai ujian anda dari database!**

# PENUTUP

Akhirnya kita sampai pada akhir presentasi ini. Bagaimanapun penulis tak merekomendasikan curang dalam ujian apapun. Presentasi ini hanya dibuat untuk hiburan karena penulis sedang Bosan. Segala trik yang penulis jelaskan berkemungkinan untuk berhasil. Walaupun tak 100%. Berbagai faktor menentukan spt versi exambro, ketersediaan alat, pengalaman anda dalam hacking dsb. Penulis bukan pamer kemampuan, sok pinter atau apa, namun hanya mencurahkan kebosanan penulis. Bahkan kalau penulis pintar, penulis tak akan menggunakan waktu 5 jam untuk menulis presentasi ini. Dan penulis tak bertanggungjawab atas segala yang ditimbulkan atas segala yang penulis jabarkan disini.

# Sumber

exambro client

manual-cbt-un-2017-kemdikbud\_111116-11.pdf

<http://www.jawaracloud.net/2016/11/cara-setting-aplikasi-unbk-2017-lengkap.html>

Ingatan dan analisa penulis