

You had an attack and now you want to know how it took place?

## ATM/IT Forensic Investigation

Most banks and other organizations will face a threat. When it comes to IT and ATM criminal investigation we can engage in such a way that we will reveal all past history of what has happened and how from deep inside the software/operating system and device logs, find evidence against the perpetrator and propose solutions on how to avoid similar situations in the future.

As criminals are attracted by large corporations and specially by banks we know their usual ways of trying to infiltrate to your systems. This service is used when you have situations that require an IT or ATM/IT type of forensic investigation.



Take for example a situation where you have missing cash from ATMs. There we can examine past logs either paper or electronic or both in order to find times of access, sensor activity, connection status and many more information that can reveal what exactly happened to your system helping to reveal the truth. Another example is when perpetrators try to do skimming on your ATMs and you want to identify how it was done.

```

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer]
"Build"="91058b"
"IntegratedBrowser"=dword:00000001
"MKEnabled"="Yes"
"svcKBFWLink"="http://go.microsoft.com/fwlink/?LinkId=692162"
"svcKBNumber"="K83104002"
"svcUpdateVersion"="11.0.26"
"svcVersion"="11.63.1058b.0"
"Version"="9.11.1058b.0"
"W2kVersion"="9.11.1058b.0"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\AboutURLs]
"blank"="res://mshtml.dll/blank.htm"
"DesktopItemNavigationFailure"="res://ieframesticky.dll/navcancl.htm"
"Home"=dword:0000010e
"InProgress"="res://ieframe.dll/inprivate.htm"
"NavigationCanceled"="res://ieframe.dll/navcancl.htm"
"NavigationFailure"="res://ieframe.dll/navcancl.htm"
"NoAdd-ons"="res://ieframe.dll/noaddon.htm"
"NoAdd-onsInfo"="res://ieframe.dll/noaddoninfo.htm"
"PostNotCached"="res://ieframe.dll/repost.htm"
"SecurityRisk"="res://ieframe.dll/securityatrisk.htm"

```

**ALERT**  
Security violation  
invalid file

### The Service Deliverables:

- Analysis of Hard drives of ATMS and users
- Analysis of infiltrated ATM logs and Switch logs
- Analysis of routers
- Analysis of systems logs for access
- Analysis of physical surveillance systems data
- Interviewing possible witnesses
- Report of findings

### **CORE PROCESS**

P.O.Box 28184  
2091 STROVOLOS  
NICOSIA  
CYPRUS

Tel. 357 22 106 847  
info@thecoreprocess.com  
www.thecoreprocess.com