The Development of a Modular Software Framework for a Distributed Forensic Attack Profiling Network

George Chlapoutakis, Angus Marshall & Phil Brooke

INTRODUCTION

Forensic Profiling has been used in traditional criminal investigations but effort has only recently been made to apply the same principles to Criminal Investigations of Digital Crimes.

1.Profiling across disciplines

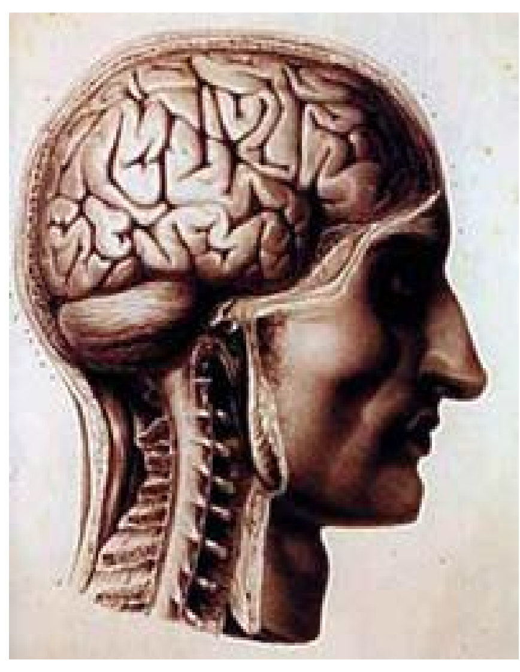


Figure 1

1.1. Profiling in Criminal Investigations:

Profiling has been extensively used in Criminal Investigations to give a working description of an offender based on analysis of different factors specific to the case and their comparison to known characteristics, personality types and mental issues of perpetrators of similar offences.

1.2. Profiling in Computer Networking:

In Networking profiling has been used to analyse network traffic flow so as to understand and identify network traffic issues and classify network traffic by applications used.

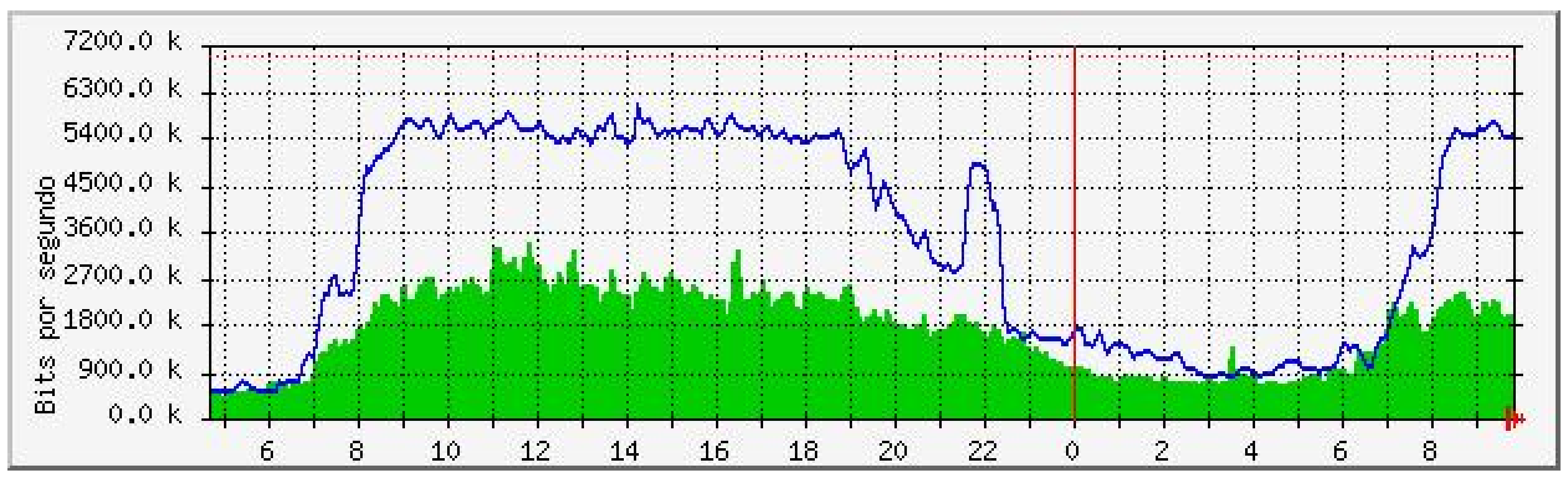
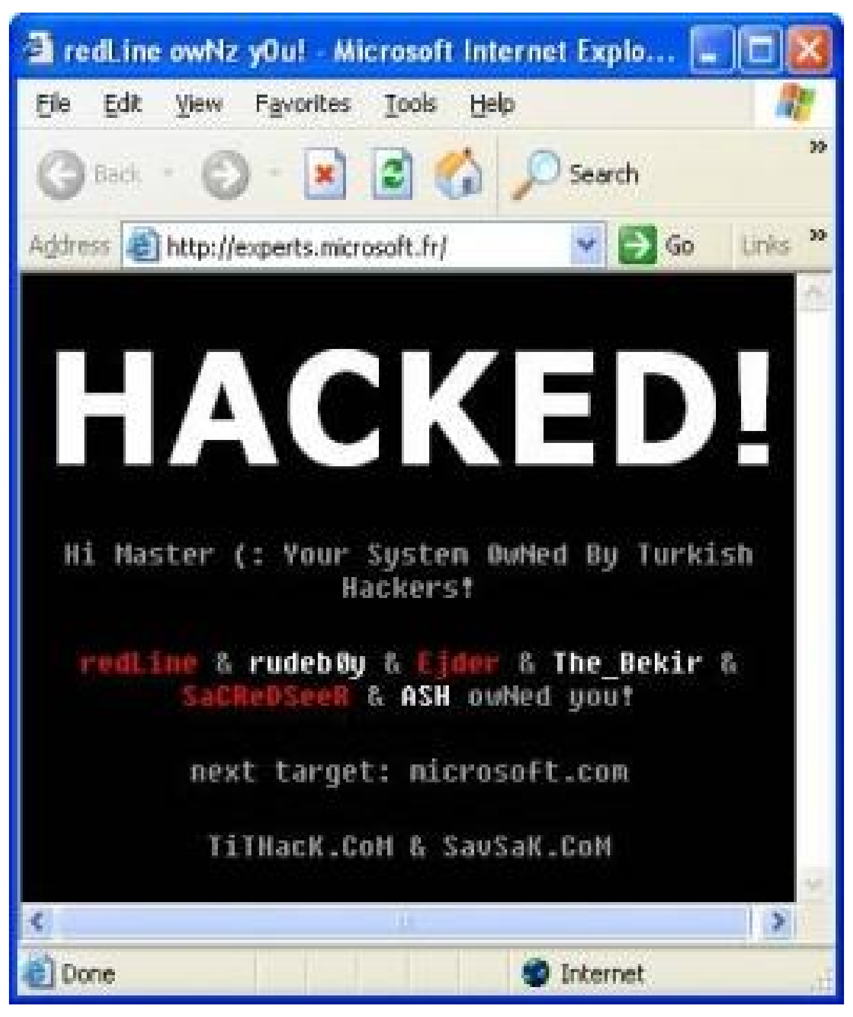


Figure 2: Sample network traffic

1.3. Profiling in Network Security:

In Network Security & Intrusion Detection, profiling has been used to correlate multiple sources of information to detect intrusions on computer systems and Distributed Denial of Service attacks on computer networks.



redLine owNz yOu! - Microsoft Internet Explo...

http://experts.microsoft.fr/

HACKED!

Hi Master (: Your System OwNed By Turkish Hackers!

redLine & rudeb0y & Ejder & The_Bekir & SaCReDSeeR & ASH owNed you!

next target: microsoft.com

TiTHacK.CoM & SavSaK.CoM

Figure 3: Microsoft's French website hacked

2. Forensic Network Attack Profiling in Digital Investigations

2.1. Why Intrusion Detection Systems cannot do the job forensically:

- Intrusion Detection Systems are not designed with integrity protection or evidential reasoning.
- Are admissible as evidence in a court only for their ability to signify the presence of the accused attacker in a computer or network.

2.2. Proposed Distributed Forensic Attack Profiling Network:

- Software Framework → Modular Design for Distributed Sensors
- Workstations act as sensors → Distributed data pre-processing
- Analysis & Correlation: Centralised, further processing of data
- Produces: Attacker Profile report → Admissible as evidence in court

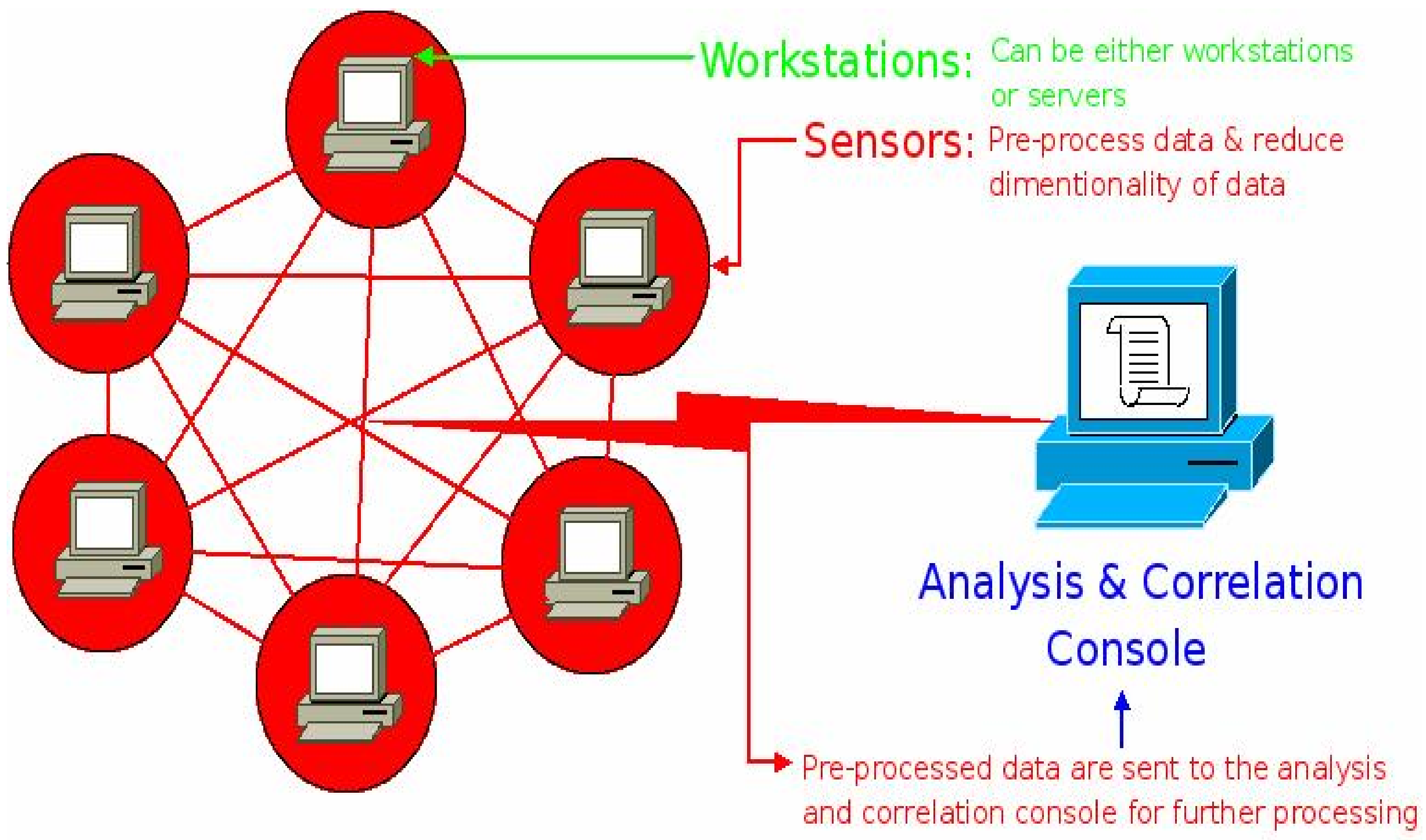

Workstations:
Can be either workstations or servers
Sensors:
Pre-process data & reduce dimentionality of data
Analysis & Correlation Console
Pre-processed data are sent to the analysis and correlation console for further processing

Figure 4: The structure of the Forensic Profiling Network

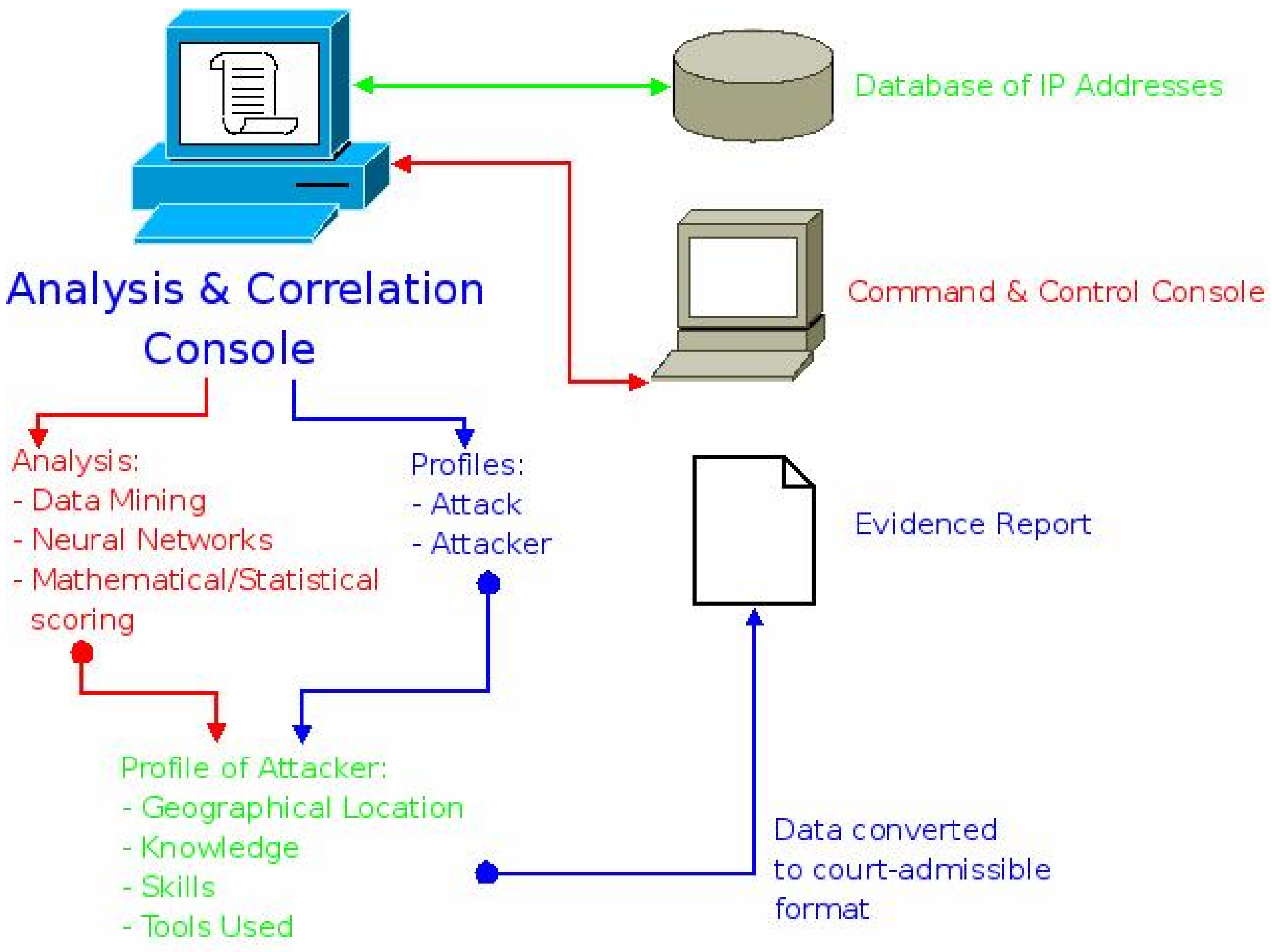


Figure 5: Operations of the Analysis And Correlation Console

3. Discussion

- The proposed approach combines elements of Intrusion Detection theory, Network Profiling, Data Mining, Artificial Neural Networks and BotNet technologies to form a Distributed Forensic Attack Profiling Network tool.
- Its framework model will use a collection of generalised modules to easily assemble customised sensors to allow for customised network traffic data collection.
- This will result in secure and real-time profiling of host and network-based attacks and the individuals behind the attacks.

Cited Figures

Figure 1: http://www.forensic-science.com/profiling.jpg
Figure 2: http://www.acm.org/crossroads/xrds10-1/gfx/daily_traffic.png
Figure 3: http://www.acunetix.com/news/microsoft_france2.jpg

School of Science and Technology

UNIVERSITY OF TEESSIDE

Digital Forensics Group, School of Science & Technology