Is Digital Forensics a Science?

The 1st International Conference on Digital Forensics and Investigation

Michael Kwan (关煜群)
Vice President
Information Security & Forensics Society
Is Digital Forensic a Science

How Scientific is Today’s Digital Forensic

Event Reconstruction & Conclusion

Forensic Science

Digital Forensic
Forensic science is science used for the purpose of the law.
What is “Science”

Science is a collection of systematic methodologies used to increasingly understand the world.

*Forensic Science: Modern Methods of Solving Crime,*
Max M. Houck

科学是帮助理解世界的系统的方法
Forensic Science is a Historical Science

- Events (crimes) have occurred in the past (犯罪)事件是已发生的
- You did not witness the crime as it occurs 事件发生时，您并没有目击到
- Identify and analyze the traces left behind 识别并分析留下的足迹
- Interpret the actions of perpetrator & victim, formulate forensic conclusion 解析罪犯&受害者的行，陈述取证结论
Where the “Trace” come from

Locard’s Exchange Principle

Every contact leaves a trace; when 2 things come into contact, information exchange
每一次联系都会留下踪迹；当两个事物发生关联时，必然有信息的交换。

The traces reveal associations between people, places and things
踪迹揭示了人物、地点、事件之间的相关性

These associations can only be obtained by interpretation of traces
这些相关性只能通过“解析”踪迹而获得
Interpretation & Scientific Method

It is the interpretation of the data collected through the scientific method that leads to knowledge. Mere collection of data means nothing.

Mere guess or personal opinion is not interpretation. Interpretation is a mixture of inductive and deductive inferences through the use of the scientific method.

Bloodstain Pattern Analysis
T. Bevel & R. Gardner
Deductive inference is that the conclusion must be true if the premise is true.

推论：若前提是真实的，其结论必然是真实的。

Inductive inference is that the conclusion is likely to be true if the premise is true.

归纳：若前提是真实的，其结论有可能是真实的。
**Deductive and Inductive Inferences**

If “Crime A” is true, then “Trace B” is true (i.e. “Crime A” is causal event to “Trace B”)
如果罪行A是真，那么踪迹B是真（即罪行A是踪迹B的诱因）

### Deductive Inference

<table>
<thead>
<tr>
<th>A is true</th>
<th>B is false</th>
</tr>
</thead>
<tbody>
<tr>
<td>Therefore B is true (conclusion)</td>
<td>Therefore A is false (conclusion)</td>
</tr>
</tbody>
</table>

### Inductive Inference

<table>
<thead>
<tr>
<th>B is true</th>
</tr>
</thead>
<tbody>
<tr>
<td>Therefore A becomes plausible (conclusion)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A is false</th>
</tr>
</thead>
<tbody>
<tr>
<td>Therefore B becomes less plausible (conclusion)</td>
</tr>
</tbody>
</table>
Scientific Method

- Identify the problem to be resolved
  确定待解决的问题
- Collect & gather data that may establish an answer to the question
  收集可能与答案有关的数据
- Posit hypothesis regarding the problem
  设立该问题的假设
- Classify & organize the collected data for interpretation
  分类整理收集的数据以作解析
- Test the hypothesis by comparing expectations for a given hypothesis against the observed data
  通过对比预期结果和观察数据来测试假设
- Draw a conclusion from the information examined
  通过调查的信息得出结论
Is Digital Forensic a Science

How Scientific is Today’s Digital Forensic

Event Reconstruction & Conclusion

Digital Forensic

Forensic Science
What is “Digital Forensic”

• No difference to traditional forensic science – A historical science
与传统取证科学无差异

• Identify and analyze the digital traces left behind
识别并分析留下的电子踪迹

• Interpret the actions of perpetrator & victim, formulate forensic conclusion
解析罪犯与受害者的行动，陈述取证结论
Locard’s Exchange Principle & Digital Traces

Locard’s Exchange Principle also applies to Digital Traces

**Computer Generated Record** 电脑生成记录
Shows computer processes that have been performed, e.g. system logs
体现计算机运行记录，如：系统日志

**Computer Stored Record** 电脑存储记录
Shows user’s actions performed on created files e.g. date & time stamps
体现创建文件时的用户行为，如：时间戳
The Processes of Digital Forensics

Identification
- Crime scene management
- Data search
- Identify evidential data

Preservation
- Securing evidence
- Imaging
- Data protection

Analysis
- Analysis all related evidence
- Data correlation
- Event reconstruct

Presentation
- Forensics report – hypotheses & conclusion
- Testimony – expert opinion

Search & Handling of Evidence
- 搜索&处理数据

Analysis & Conclusion
- 分析&结论
Is Digital Forensic a Science

How Scientific is Today’s Digital Forensic

Event Reconstruction & Conclusion

Forensic Science

Digital Forensic

事件重构&结论

取证科学

数字取证
Event Reconstruction Processes

- The crime is indeed an **incident** 犯罪是一种事故
- An **incident** is made up of **events** 某一事故由多个事件构成
- An **event** is comprising of specific **actions**, which turn out to be the **traces** or **evidence** 某一事件由多个特殊行为构成，行为体现为踪迹或证据

Event reconstruction is “walk-back” processes
事件重构是“回溯”这些过程

Traces $\rightarrow$ Event

Reconstructed Event $\rightarrow$ Incident (Crime)
How to Achieve Event Reconstruction

- Identify incident and related events 鉴定事故及相关事件
- Identify traces that are caused by the event 鉴定事件所引发的踪迹

- Collect data and establish the likely events that could have caused the data 收集数据并构建引发这些数据的可能性事件
- Consider these events in relationship to one another to establish the order of sequence 综合考虑事件相关性，并建立其发生的顺序
- If contradictory sequence existed, analyze and determine which is more probable 若存在矛盾的顺序，需评审证据并判断哪一个的可能性更大
- Flow chart the overall incident based on the events and their determined sequence 基于事件及确定的顺序，规划出整个事故的流程图
The seized computer was the 1st *seeder* distributing the pirated movie via BT network.

获取的计算机是第一个通过BT网络分发侵犯版权电影的*seeder*。
**Event Reconstruction Processes of the BT Case**

**HYPOTHESES:**

- **H**: The seized computer was used as the initial seeder to share the pirated file on a BitTorrent network.
- **H₁**: The pirated file was copied from the seized optical disk to the seized computer.
- **H₂**: A torrent file was created from the copied file.
- **H₃**: The torrent file was sent to newsgroups for publishing.
- **H₄**: The torrent file was activated, which caused the seized computer to connect to the tracker server.
- **H₅**: The connection between the seized computer and the tracker was maintained.
Event Reconstruction Processes of the BT Case

EVIDENCE:

E1 Modification time of the destination file equals that of the source file
E2 Creation time of the destination file is after its own modification time
E3 Hash value of the destination file matches that of the source file
E4 BitTorrent client software is installed on the seized computer
E5 File link for the shared file is created
E6 Shared file exists on the hard disk
E7 Torrent file creation record is found
E8 Torrent file exists on the hard disk
E9 Peer connection information is found
E10 Tracker server login record is found
E11 Torrent file activation time is corroborated by its MAC time and link file
E12 Internet history record about publishing website is found
E13 Internet connection is available
E14 Cookie of the publishing website is found
E15 URL of the publishing website is stored in the web browser
E16 Web browser software is available
E17 Internet cache record about the publishing of the torrent file is found
E18 Internet history record about the tracker server connection is found
Is Digital Forensic a Science

How Scientific is Today’s Digital Forensic

数字取证其科学性
What Most Digital Forensic Examiners Doing Today

Identification  
Preservation  
Analysis  
Presentation

- Securing evidence
- Imaging
- Data protection
- Crime scene management
- Data search
- Identify evidential data
- Analysis all related evidence
- Data correlation
- Event reconstruct
- Forensics report – hypotheses & conclusion
- Testimony – expert opinion

Using forensic tools – the “Click Button” Expert

Reporting “when’, “where”, “how” the evidence was found. No “interpretation”, “event reconstruction”. Not showing “scientific method”
The Impact of “Click Button” Approach

- Without any scientific interpretations, false-positive scenarios cannot be eliminated → easy to fabricate digital traces for the tools to find
- “Is the examination performed by the expert or the software?” → the digital forensic expert is just a technician; reliability and credibility of the expert are impeded
  “检查是由专家还是由软件完成的呢？” → 数字取证专家只是一个技术人员，难以保证专家的可靠性与可信性
It’s time to be a Digital Forensic Scientist

- Digital forensic per se is scientific
- It is the digital forensic “expert” who is not doing his/her forensic job scientifically

STOP being a “CB” expert; be a digital forensic scientist!

IF WE FAIL TO ACT NOW, WHO WILL?
Q and A