The Potential of Digital Traces in Providing Evidence at Activity Level

By
Dr. J. Henseler (University of Applied Sciences Leiden) and Prof.dr. C.J. de Poot (Amsterdam University of Applied Sciences, the Police Academy, and VU University of Amsterdam)

From the proceedings of
The Digital Forensic Research Conference
DFRWS 2020 USA
Virtual -- July 20-24

The potential of digital traces in providing evidence at activity level

Dr.ir. Hans Henseler
Professor Digital Forensics & E-Discovery,
University of Applied Sciences Leiden

Prof.dr. C.J. de Poot,
Professor of Forensic Science at the Amsterdam University of Applied Sciences and the Police Academy, and professor of Criminalistics at the VU University of Amsterdam

DFRWS 2020 Virtual USA

Contents

- Anchored narratives
- Building a story
- Classical forensic principles and digital evidence
- From trace to activity
- Case example
- Digital evidence example
- Conclusion

Ultimate goal of the investigation process

- Reconstruction of what happened
- Present a narrative about an event in the past:
  - that is coherent and believable
  - that is supported by sufficient criminal evidence

Anchored narratives: The psychology of criminal evidence, W. A. Wagenaar, P. J. van Koppen, and H. F. M. Crombag, New York: St Martin's Press and Hertfordshire: Harvester Wheatsheaf, 1993.

Anchored narratives

- Quality of the narrative:
  - "A good story is better than half of the proof"
    (plausible, coherent, logical sequence of actions)
- How the narrative is supported by the evidence:
  - The story must be anchored by "common-sense generalisations which are generally accepted as true" (E.g.: witnesses under oath usually speak the truth, or if the orientation state in KnowledgeC is vertical the phone was in a vertical position)

How do we build a story?

- Basic elements of the story come from answers to seven golden criminalistic Wh-Questions
- Framework for the reconstruction:
  - Who – was involved?
  - What – happened?
  - Where – did it happen?
  - When – did the crime take place?
  - What with – was the crime committed?
  - in What way – was the crime committed (how)?
  - Why – was the crime committed?

c

Classical forensic principles in digital evidence

- **Transfer** of matter
  - When a person/object touches another person/object
  - Digital evidence: transfer of information during interaction
- **Divisibility** of matter
  - A part has the same properties as the whole
  - Digital evidence: can be replicated / duplicated as much as needed

Digital Evidence

- Identification of sources that carry digital evidence:
  - Where do you have to search?
  - What kind of information could be found?
  - Why is it relevant? How can you link it to an event?
- Analysis of digital evidence will fail without proper identification.
  - necessary to understand the system and its architecture to understand what you see and what you can find
  - not about tools, but about understanding how activities leave digital traces

Physical traces

- Events only have limited physical consequences
- Physical consequences can often be caused by a variety of events
- Physical traces are used to:
  - form hypotheses,
  - validate reconstructions that follow from other traces

Source level vs Activity level

- Traditionally, forensic investigation has primarily focused on determining the **source** of the trace (who left the trace)
- Recently, forensic investigation has also started addressing the question **how** traces were left, and if traces are related to the crime.
- In this respect, physical traces have limited value…

Deriving activities from traces

- Question changes from: ‘Who is the source of the trace’ to ‘what activity led to the deposition of the trace?’

Digital evidence & Activity level

- Digital evidence contains more information about activities than physical traces:
  - information about exact moments in time, sequence of events and location can be derived from digital evidence
  - Sometimes communication information contains both content as well as activity:
    - Nature of a conversation or from search terms that were entered can be placed in time.
- Experiments are needed to investigate how and where activities are registered and leave digital traces

Case: murder on the Bûterwei

NLTIMES.NL TOP STORIES CRIME POLITICS BUSINESS SPORTS FOOD HEALTH WEIRD TECHNOLOGY ENTERTAIN

CRIME TOP STORIES

MAN FOUND MURDERED AFTER MUSIC FESTIVAL IN FRIESLAND VILLAGE

By Janene Pieters on July 10, 2017 - 08:29

Police. (Photo: Politie / -)

A body was found in a meadow in the Friesland village of De Westereen on Sunday morning. The victim was identified as 37-year-old Tjeerd van Seggeren from Kollumerzwaag. The police are still investigating, but the initial conclusion is that the man was killed in a crime.

https://nltimes.nl/2017/07/10/man-found-murdered-music-festival-friesland-village

deVolkskrant

RECONSTRUCTIE MOORD OP DE BÛTERWEI

Hoe Google-data in een moordzaak leidden naar de echtgenote

De moord op een vader van drie kinderen stelt de recherche aanvankelijk voor raadsels. Dankzij gegevens van Google komt het tot een veroordeling van de vrouw van het slachtoffer.

Huib Modderkolk

https://www.volkskrant.nl/nieuws-achtergrond/hoe-google-data-in-een-moordzaak-leidden-naar-de-echtgenote~b092755e

de Rechtspraak

Home Onderwerpen Uitspraken en nieuws Registers de Rechtspraak

Rechtbank Noord-Nederland > Nieuws > 20 jaar celstraf voor moord op echtgenoot

20 jaar celstraf voor moord op echtgenoot

Leeuwarden, 11 juli 2019

De rechtbank Noord-Nederland, locatie Leeuwarden heeft een 35-jarige uit Kollumerzwaag veroordeeld tot twintig jaar gevangenisstraf voor de moord op haar echtgenoot Tjeerd van Seggeren op 9 juli 2017.

Ontkennende verdachte

https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Noord-Nederland/Nieuws/Paginas/20-jaar-celstraf-voor-moord-op-echtgenoot.aspx

Scenarios in the Bûterwei case

Scenario Defense	Scenario Prosecutor	Evidence
Suspect claims not to have left on the evening before the murder	Around 10pm the suspect has driven her car to a nearby village, drives a bit further, stops at the side of the road, turns around and drives home	Google-timeline from Google Cloud that was collected with a password that was recovered from the iPhone from the suspect.
Phone from the suspect was switched of because the battery was emtpy.	Suspect manually turned off her phone.	Logfiles in the phone show that the battery was not empty (throttling status).
Suspect has asked the victim to meet her at the Bûterwei. When the suspect arrive at the agreed meeting place she didn't see the victim and turned home.	Suspect has asked the victim to meet her at the Bûterwei. She met the victim and walked with him into the field where he was subsequently murdered.	Google Cloud data indicate that the phone of the victim was still moving at 00:12am. At 00:40am the orientation of the phone alters considerable and at 00:43am there is no further movement. The phone is at the location where the victim is found the next morning. Location data from both phones confirm that they have been within a distance of 15-20 meters.
Suspect has called the victim during the search at night.	Suspect hasn't called the victim during the search at night.	Call history of the phone of the suspect does not contain outgoing calls during the search.
After not finding her husband, the suspect drove home directly at a speed of 80 km/hr.	Suspect didn't drive home directly but stopped along the way.	Security camera along the route indicate that the average speed of the suspects car was 15 km/hr.

Scenarios in the Bûterwei case

Scenario Defense	Scenario Prosecutor	Evidence
Suspect claims not to have left on the evening before the murder	Around 10pm the suspect has driven her car to a nearby village, drives a bit further, stops at the side of the road, turns around and drives home	Google-timeline from Google Cloud that was collected with a password that was recovered from the iPhone from the suspect.
Phone from the suspect was switched of because the battery was emtpy.	Suspect manually turned off her phone.	Logfiles in the phone show that the battery was not empty (throttling status).
Suspect has asked the victim to meet her at the Bûterwei. When the suspect arrive at the agreed meeting place she didn't see the victim and turned home.	Suspect has asked the victim to meet her at the Bûterwei. She met the victim and walked with him into the field where he was subsequently murdered.	Google Cloud data indicate that the phone of the victim was still moving at 00:12am. At 00:40am the orientation of the phone shows considerable and at 00:43am there is no further movement. The phone is at the location where the victim is found the next morning. Location data from both phones confirm that they have been within a distance of 15-20 meters.
Suspect has called the victim during the search at night.	Suspect hasn't called the victim during the search at night.	Call history of the phone of the suspect does not contain outgoing calls during the search.
After not finding her husband, the suspect drove home directly at a speed of 80 km/hr.	Suspect didn't drive home directly but stopped along the way.	Security camera's along the route indicate that the average speed of the suspects car was 15 km/hr.

Scenarios in the Bûterwei case

Scenario Defense	Scenario Prosecutor	Evidence
Suspect claims not to have left on the evening before the murder	Around 10pm the suspect has driven her car to a nearby village, drives a bit further, stops at the side of the road, turns around and drives home	Google-timeline from Google Cloud that was collected with a password that was recovered from the iPhone from the suspect.
Phone from the suspect was switched of because the battery was emtpy.	Suspect manually turned off her phone.	Logfiles in the phone show that the battery was not empty (throttling status).
Suspect has asked the victim to meet her at the Bûterwei. When the suspect arrive at the agreed meeting place she didn't see the victim and turned home.	Suspect has asked the victim to meet her at the Bûterwei. She met the victim and walked with him into the field where he was subsequently murdered.	Google Cloud-data inidicates that the phone of the victim was still moving at 00:27am. At 00:40am the orientation of the phone alters considerable and at 00:43am there is no further movement. The phone is a the location where the victim is found the next morning. Location date from both phones confirm that they have been within a distance of 15-20 meters.
Suspect has called the victim during the search at night.	Suspect hasn't called the victim during the search at night.	Call history of the phone of the suspect does not contain outgoing calls during the search.
After not finding her husband, the suspect drove home directly at a speed of 80 km/hr.	Suspect didn't drive home directly but stopped along the way.	Security cameras along the route indicate that the average speed of the suspects car was 15 km/hr.

Scenarios in the Bûterwei case

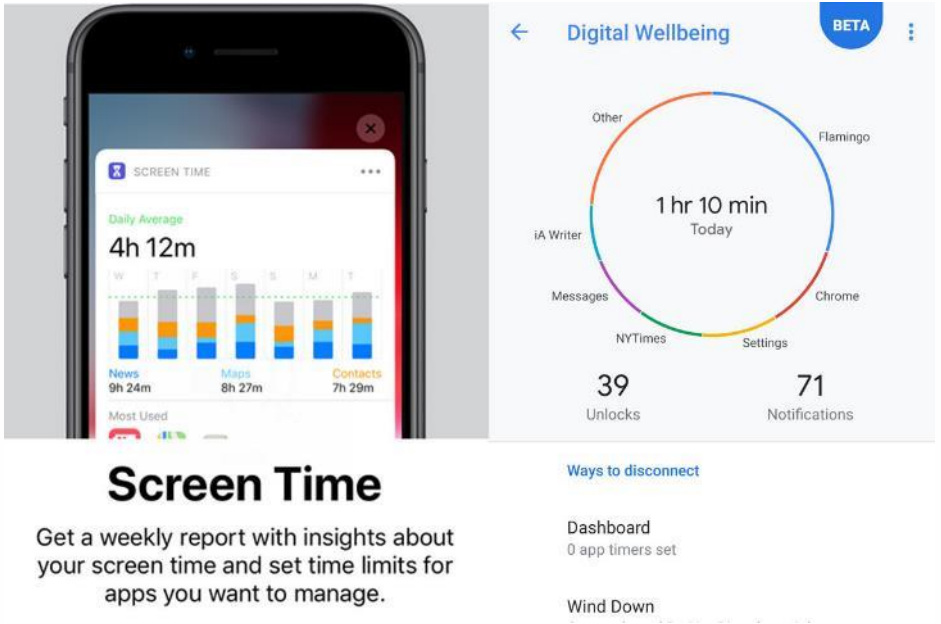
Scenario Defense	Scenario Prosecutor	Evidence
Suspect claims not to have left on the evening before the murder	Around 10pm the suspect has driven her car to a nearby village, drives a bit further, stops at the side of the road, turns around and drives home	Google-timeline from Google Cloud that was collected with a password that was recovered from the iPhone from the suspect.
Phone from the suspect was switched of because the battery was emtpy.	Suspect manually turned off her phone.	Logfiles in the phone show that the battery was not empty (throttling status).
Suspect has asked the victim to meet her at the Bûterwei. When the suspect arrive at the agreed meeting place she didn't see the victim and turned home.	Suspect has asked the victim to meet her at the Bûterwei. She met the victim and walked with him into the field where he was subsequently murdered.	Google Cloud-data inidicates that the phone of the victim was still moving at 00:27am. At 00:40am the orientation of the phone alters considerable and at 00:43am there is no further movement. The phone is a the location where the victim is found the next morning. Location date from both phones confirm that they have been within a distance of 15-20 meters.
Suspect has called the victim during the search at night.	Suspect hasn't called the victim during the search at night.	Call history of the phone of the suspect does not contain outgoing calls during the search.
After not finding her husband, the suspect drove home directly at a speed of 80 km/hr.	Suspect didn't drive home directly but stopped along the way.	Security cameras along the route indicate that the average speed of the suspects car was 15 km/hr.

Scenarios in the Bûterwei case

Scenario Defense	Scenario Prosecutor	Evidence
Suspect claims not to have left on the evening before the murder	Around 10pm the suspect has driven her car to a nearby village, drives a bit further, stops at the side of the road, turns around and drives home	Google-timeline from Google Cloud that was collected with a password that was recovered from the iPhone from the suspect.
Phone from the suspect was switched of because the battery was emtpy.	Suspect manually turned off her phone.	Logfiles in the phone show that the battery was not empty (throttling status).
Suspect has asked the victim to meet her at the Bûterwei. When the suspect arrive at the agreed meeting place she didn't see the victim and turned home.	Suspect has asked the victim to meet her at the Bûterwei. She met the victim and walked with him into the field where he was subsequently murdered.	Google Cloud-data indicates that the phone of the victim was still moving at 00:27am. At 00:40am the orientation of the phone alters considerable and at 00:43am there is no further movement. The phone is a the location where the victim is found the next morning. Location date from both phones confirm that they have been within a distance of 15-20 meters.
Suspect has called the victim during the search at night.	Suspect hasn't called the victim during the search at night.	Call history of the phone of the suspect does not contain outgoing calls during the search.
After not finding her husband, the suspect drove home directly at a speed of 80 km/hr.	Suspect didn't drive home directly but stopped along the way.	Security cameras along the route indicate that the average speed of the suspects car was 18 km/hr.

Time trackers on Android and iPhone

- In 2018 both Apple as well as Google have started adding so call ed *time trackers* on their smartphone OS.
- Google has called this feature *Digital Wellbeing* (starting Android version 9 Pie)
- Apple has called this feature *Screen Time* (starting Apple iOS version 12)



Tip: Look up "pattern of life analysis" & "digital forensics"
Check out Sarah Edwards (APPOLO) and Alexis Brignoni

Example: Picture was taken

11/1/2019 9:41:44 AM	End Date/Time	Device interaction	Operating Syst...	KnowledgeC Screen Backlight...	State	Screen off
11/1/2019 9:41:47 AM	Recorded Date/Time	Device interaction	Operating Syst...	KnowledgeC Screen Backlight...	State	Screen off
11/1/2019 9:41:48 AM	End Date/Time	Device interaction	Operating Syst...	KnowledgeC Device Lock States	State	Locked
11/1/2019 9:41:49 AM	Recorded Date/Time	Device interaction	Operating Syst...	KnowledgeC Device Lock States	State	Locked
11/1/2019 9:41:52 AM	Start Date/Time	Device interaction	Operating Syst...	KnowledgeC Device Orientatio...	State	Vertical
11/1/2019 9:41:53 AM	Start Date/Time	Device interaction	Operating Syst...	KnowledgeC Application Focus	Application...	com.apple.camera
11/1/2019 9:41:56 AM	Start Date/Time	Device interaction	Operating Syst...	KnowledgeC Device Orientatio...	State	Sideways
11/1/2019 9:41:56 AM	End Date/Time	Device interaction	Operating Syst...	KnowledgeC Device Orientatio...	State	Vertical
11/1/2019 9:41:59 AM	Recorded Date/Time	Device interaction	Operating Syst...	KnowledgeC Device Orientatio...	State	Vertical
11/1/2019 9:42:03 AM	Date/Time		Unknown	Unknown	Date/Time -...	2019-11-01 08:42:03
11/1/2019 9:42:04 AM	End Date/Time	Device interaction	Operating Syst...	KnowledgeC Device Orientatio...	State	Sideways
11/1/2019 9:42:05 AM	Date/Time		Unknown	Unknown	Sender	FA4F3997-EEB7-4A2A-
11/1/2019 9:42:05 AM	Last Modified Date/Ti...	File/folder openi...	Media	Pictures	File Name	IMG_0014.JPG
11/1/2019 9:42:05 AM	Last Modified Date/Ti...	File/folder openi...	Media	Live Photos	File Name	IMG_0014.JPG
11/1/2019 9:42:05 AM	Last Modified Date/Ti...	File/folder openi...	Media	Videos	File Name	IMG_0014.MOV
11/1/2019 9:42:05 AM	Modified	File/folder openi...	File system	File		IMG_0014.JPG
11/1/2019 9:42:05 AM	Modified	File/folder openi...	File system	File		IMG_0014.MOV
11/1/2019 9:42:06 AM	End Date/Time	Device interaction	Operating Syst...	KnowledgeC Application Focus	Application...	com.apple.camera

Timeline with activities originating from, among other things, the KnowledgeC tables from which, based on technical facts, it appears that a photo was taken with the telephone.

Example: Picture was downloaded

8/29/2016 19:15:38 PM	Date Visited Date/Time	Browser usage	Web Related	Chrome Web Visits	URL	https://mail.google.com/mail/#inbox
8/29/2016 19:15:41 PM	Date Visited Date/Time	Browser usage	Web Related	Chrome Web Visits	URL	https://out.reddit.com/t3_4yxb3z?url=https%3
8/29/2016 19:15:41 PM	Date/Time	Browser usage	Refined Results	Social Media URLs	Site Name	Reddit
8/29/2016 19:15:41 PM	Date Visited Date/Time	Browser usage	Web Related	Chrome Web Visits	URL	https://drscdn.500px.org/photo/168898645/q:
8/29/2016 19:15:41 PM	Last Visited Date/Time	Browser usage	Web Related	Chrome Web History	URL	https://out.reddit.com/t3_4yxb3z?url=https%3
8/29/2016 19:15:41 PM	Last Visited Date/Time	Browser usage	Web Related	Chrome Web History	URL	https://drscdn.500px.org/photo/168898645/q:
8/29/2016 19:15:41 PM	Date/Time	Browser usage	Refined Results	Social Media URLs	Site Name	Reddit
8/29/2016 19:15:47 PM	Last Accessed Date/Time	File/folder opening	Media	Pictures	File Name	stock-photo-168898645.jpg
8/29/2016 19:15:47 PM	Start Time Date/Time	File download	Web Related	Chrome Downloads	Download Source	https://drscdn.500px.org/photo/168898645/q:
8/29/2016 19:15:47 PM	Target File Last Accessed Date/Time	File/folder opening	Operating System	Jump Lists	App ID	5f7b5f1e01b83767

Timeline with activities that show that a photo file has been downloaded by a user after reading an email in the Gmail inbox.

Conclusion

- Digital traces can provide evidence about the activity level of events.
- Digital traces are valuable for developing and evaluating scenarios.
- Scenarios can help in selecting and prioritizing digital traces.
- Digital forensic experts are experts in the analysis of digital traces, but digital traces are everywhere, …
- Other detectives and forensic experts need to develop a basic understanding of digital evidence so that they can utilise the information that is revealed by digital traces

Thank you for your attention

henseler.h@hsleiden.nl

www.linkedin.com/in/henseler/