An automated timeline reconstruction approach for digital forensic investigations

Dr Chris Hargreaves & Jony Patterson
Making Sense
Enhancing Investigative Capability Through Science & Technology
Research Aim

• Part of the project is concerned with providing a ‘gist’ of various data sources
  • documents
  • images
  • videos
Research Aim

• What is the ‘gist’ of a hard drive?
  • gallery view of pictures
  • proportion of the disk that are system files, images, videos etc.
  • list of email addresses
  • ...

Summary of a hard drive?

“What is the event history of this computer?”
Research Aim
Summary

• Needs to provide a ‘gist’ - a ‘summary of activity on the disk’

• Need an event reconstruction tool that produces ‘human understandable events’

• Needs to satisfy forensic requirements, particularly traceability, repeatability

• Needs to be extensible, i.e. allow the community to add

  • EnScript, RegRipper, Volatility
Existing timeline tools
Aftertime

Existing Work on Timelines: Cyber Forensic Time Lab (CFTL)

Overview of our approach

- disk image
- low-level event database
- high-timeline

XML

SQLite

Disk image
Software Components

- Low level events
- Low level timelines
- High level events
- High level timelines
- Case management
- Time converters
- File system/disk image access
- Utilities e.g logging
Low-level time extraction

Extractor Manager
(file name, path, content)

Bridge

Parser
Extractor Manager can match on file name/path

```python
elif file_name_and_path[-11:] == "_CACHE_MAP_":
    logging.debug("%s is a Firefox Cache Map. Running parser..." % file_name_and_path)
    firefox_extractor = FirefoxCacheBridge.FirefoxCacheTimeExtractor(file_name_and_path, mount_path, evidence)
    firefox_event_timeline = firefox_extractor.GetTimes()
    logging.debug("Extracted %d events from %s" % (len(firefox_event_timeline), file_name_and_path))
    return firefox_event_timeline
```
Extractor Manager can match on file signature

```python
elif file_header[0:4] == b"\xFF\xD8\xFF\xE1" or file_header[0:4] == b"\xFF\xD8\xFF\xE0":
    logging.debug("TimeExtractor found an jpg file (%s)" % file_name_and_path)
    jpg_file_extractor = EXIFBridge.EXIFTimeExtractor(file_name_and_path,
                                                       mount_path, evidence)
    jpg_file_event_timeline = jpg_file_extractor.GetTimes()
    logging.debug("Extracted %d events from %s" % (len(jpg_file_event_timeline),
                                                      file_name_and_path))
return jpg_file_event_timeline
```
## Low-level event format

<table>
<thead>
<tr>
<th>id</th>
<th>258920</th>
</tr>
</thead>
<tbody>
<tr>
<td>min_date_time</td>
<td>1301136207.4043</td>
</tr>
<tr>
<td>max_date_time</td>
<td>1301136207.4043</td>
</tr>
<tr>
<td>evidence</td>
<td>CH-TestImage2</td>
</tr>
<tr>
<td>plugin</td>
<td>Registry Parser</td>
</tr>
<tr>
<td>type</td>
<td>Last Updated</td>
</tr>
<tr>
<td>path</td>
<td><code>/Software/Microsoft/Internet Explorer/TypedURLs</code></td>
</tr>
<tr>
<td>device</td>
<td>CH-TestImage2</td>
</tr>
<tr>
<td>keys</td>
<td>(“url1”:“<a href="http://www.google.co.uk%E2%80%9D">http://www.google.co.uk”</a>)</td>
</tr>
</tbody>
</table>
Low-level event format: provenance

<table>
<thead>
<tr>
<th><strong>dataprov_source</strong></th>
<th>/Users/Chris/NTUSER.DAT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dataprov_type</strong></td>
<td>offset</td>
</tr>
<tr>
<td><strong>dataprov_value</strong></td>
<td>274784</td>
</tr>
</tbody>
</table>
Currently identified data provenance

- **offset**, e.g. in a Registry hive, index.dat, $mft
- **sql statement**, e.g. places.sqlite
- **line number**, e.g. setupapi.log
We have a SQLite database containing millions of low-level events.

<table>
<thead>
<tr>
<th>id</th>
<th>min_date_time</th>
<th>max_date_time</th>
<th>evidence</th>
<th>plugin</th>
<th>type</th>
<th>path</th>
<th>dataprov_source</th>
<th>dataprov_type</th>
<th>dataprov_val</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Created</td>
<td>/SMFT</td>
<td>/SMFT</td>
<td>offset</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Modified</td>
<td>/SMFT</td>
<td>/SMFT</td>
<td>offset</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Entry Modified</td>
<td>/SMFT</td>
<td>/SMFT</td>
<td>offset</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Accessed</td>
<td>/SMFT</td>
<td>/SMFT</td>
<td>offset</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Created</td>
<td>/SMFTMrr</td>
<td>/SMFT</td>
<td>offset</td>
<td>1024</td>
</tr>
<tr>
<td>5</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Modified</td>
<td>/SMFTMrr</td>
<td>/SMFT</td>
<td>offset</td>
<td>1024</td>
</tr>
<tr>
<td>6</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Entry Modified</td>
<td>/SMFTMrr</td>
<td>/SMFT</td>
<td>offset</td>
<td>1024</td>
</tr>
<tr>
<td>7</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Accessed</td>
<td>/SMFTMrr</td>
<td>/SMFT</td>
<td>offset</td>
<td>1024</td>
</tr>
<tr>
<td>8</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Created</td>
<td>/SLogFile</td>
<td>/SMFT</td>
<td>offset</td>
<td>2048</td>
</tr>
<tr>
<td>9</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Modified</td>
<td>/SLogFile</td>
<td>/SMFT</td>
<td>offset</td>
<td>2048</td>
</tr>
<tr>
<td>10</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Entry Modified</td>
<td>/SLogFile</td>
<td>/SMFT</td>
<td>offset</td>
<td>2048</td>
</tr>
<tr>
<td>11</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Accessed</td>
<td>/SLogFile</td>
<td>/SMFT</td>
<td>offset</td>
<td>2048</td>
</tr>
<tr>
<td>12</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Created</td>
<td>/Volume</td>
<td>/SMFT</td>
<td>offset</td>
<td>3072</td>
</tr>
<tr>
<td>13</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Modified</td>
<td>/Volume</td>
<td>/SMFT</td>
<td>offset</td>
<td>3072</td>
</tr>
<tr>
<td>14</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Entry Modified</td>
<td>/Volume</td>
<td>/SMFT</td>
<td>offset</td>
<td>3072</td>
</tr>
<tr>
<td>15</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Accessed</td>
<td>/Volume</td>
<td>/SMFT</td>
<td>offset</td>
<td>3072</td>
</tr>
<tr>
<td>16</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Created</td>
<td>/SAAttrDef</td>
<td>/SMFT</td>
<td>offset</td>
<td>4096</td>
</tr>
<tr>
<td>17</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Modified</td>
<td>/SAAttrDef</td>
<td>/SMFT</td>
<td>offset</td>
<td>4096</td>
</tr>
<tr>
<td>18</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Entry Modified</td>
<td>/SAAttrDef</td>
<td>/SMFT</td>
<td>offset</td>
<td>4096</td>
</tr>
<tr>
<td>19</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Accessed</td>
<td>/SAAttrDef</td>
<td>/SMFT</td>
<td>offset</td>
<td>4096</td>
</tr>
<tr>
<td>20</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Created</td>
<td>/S8itmap</td>
<td>/SMFT</td>
<td>offset</td>
<td>6144</td>
</tr>
<tr>
<td>21</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Modified</td>
<td>/S8itmap</td>
<td>/SMFT</td>
<td>offset</td>
<td>6144</td>
</tr>
<tr>
<td>22</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Entry Modified</td>
<td>/S8itmap</td>
<td>/SMFT</td>
<td>offset</td>
<td>6144</td>
</tr>
<tr>
<td>23</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Accessed</td>
<td>/S8itmap</td>
<td>/SMFT</td>
<td>offset</td>
<td>6144</td>
</tr>
<tr>
<td>24</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Created</td>
<td>/S8root</td>
<td>/SMFT</td>
<td>offset</td>
<td>7168</td>
</tr>
<tr>
<td>25</td>
<td>1300991498.468</td>
<td>1300991498.468</td>
<td>HC-TechCom</td>
<td>MFT</td>
<td>Modified</td>
<td>/S8root</td>
<td>/SMFT</td>
<td>offset</td>
<td>7168</td>
</tr>
</tbody>
</table>

select ", rowid "NAVICAT_ROWID" from "main"."events" limit 0,1000
Automated Analysis
Analysis Concept
(simple)

hypothesis trigger event

low level timeline

high level timeline
Analysis Concept
(slightly more complex)

- **hypothesis trigger event**
- **supporting event(s) of interest**

Low level timeline:

High level timeline:
Simple test events

flickr_search_test = PyDFT.Core.LowLevelEvent.LowLevelEvent()
flickr_search_test.type = "URL Visit"
flickr_search_test.path = "http://www\.flickr\.com/search/\?q=(\^[^&]+)"
Events can be directly compared
...but searches are more powerful if you can use regex

```python
def Match(self, test_event):
    """Tries to match a test event with the current event and returns true if they match""
    if not re.search(test_event.evidence, self.evidence):
        return None
    if not re.search(test_event.type, self.type):
        return None
    if not re.search(test_event.plugin, self.plugin):
        return None
    if re.search(test_event.path, self.path) == None:
        return None
    if test_event.event_provenance.source != None:
        if not re.search(test_event.event_provenance.source, self.event_provenance.source):
            return None
    if test_event.event_provenance.type != None:
        if not re.search(test_event.event_provenance.type, self.event_provenance.type):
            return None
    if test_event.event_provenance.value != None:
        if not re.search(test_event.event_provenance.value, self.event_provenance.value):
            return None
    for each_test_key in test_event.keys:
        # if key does not exist...
        if each_test_key not in self.keys:
            return None
        # if key data does not match...
        if not re.search(test_event.keys[each_test_key], self.keys[each_test_key]):
            return None
    else:
        return True
```
Basic Event Matching
def AmazonSearches(low_timeline, queue, start_id, end_id):

test_events_dict = GetAmazonTestEvents()
trigger_matches_from_low_timeline = low_timeline.FindMatchingEventsInRange(start_id, end_id, test_events_dict)

high_level_timeline = PyDFT.Core.HighLevelTimeline.HighLevelTimeline()

for each_low_event in trigger_matches_from_low_timeline:
    matched_trigger = each_low_event.MatchAnyTestEvent(test_events_dict)
    if matched_trigger:
        # make high level event
        high_event = PyDFT.Core.HighLevelEvent.HighLevelEvent()
        high_event.AddTime(each_low_event.date_time_min)
        high_event.AddTime(each_low_event.date_time_max)
        high_event.type = "Amazon search"
        high_event.category = "Web"
        high_event.evidence_source = each_low_event.evidence
        high_event.device = each_low_event.evidence

        # get search terms and other detail
        search_term = GetSearchTermFromURL(test_events_dict[matched_trigger].path, each_low_event.path)
        high_event.description = "Amazon search for '%s'" % search_term
        high_event.keys["Search term"] = search_term
        if "Page Title" in each_low_event.keys:
            high_event.keys["Page Title"] = each_low_event.keys["Page Title"]

        # Add reasoning for this high level event
        reasoning = PyDFT.Core.HighLevelEvent.ReasoningArtefact()
        reasoning.id = each_low_event.id
        reasoning.test_event = test_events_dict[matched_trigger]
        reasoning.description = "Amazon search URL found (%s)" % each_low_event.path
        high_event.trigger = reasoning

        # Add the event to the high-level timeline
        high_level_timeline.AddEvent(high_event)

queue.put(high_level_timeline)
More Complex Event Matching
Methods for matching

MatchAnyTestEvent(self, dict_of_test_events)
FindMatchingEventsInIdRange(self, start, end, test_events)
FindEventsInSubTimeline(self, event_list, start, end)
FindEventsRelatedToAPath(self, path)
# Construct the test event -- matching url
trigger_test_event = LowLevelEvent.LowLevelEvent()
trigger_test_event.type = "URL Visit"
trigger_test_event.path = "http://[a-zA-Z0-9]*?\.youtube\.com/watch\?v=([^&]+)&?(.*"

videoplayback_access_test = PyDFT.Core.LowLevelEvent.LowLevelEvent()
videoplayback_access_test.type = "Accessed"
videoplayback_access_test.path = "/Temporary Internet Files/Low/Content.IE5/(.+)/(videoplayback\[[0-9]{1}\])"

videoplayback_modify_test = PyDFT.Core.LowLevelEvent.LowLevelEvent()
videoplayback_modify_test.type = "Modified"
videoplayback_modify_test.path = "/Temporary Internet Files/Low/Content.IE5/(.+)/(videoplayback\[[0-9]{1}\])"

videoplayback_firefox_test = PyDFT.Core.LowLevelEvent.LowLevelEvent()
videoplayback_firefox_test.plugin = "Firefox Cache"
videoplayback_firefox_test.type = "Cached"
videoplayback_firefox_test.keys["url"] = ".*?youtube.com/videoplayback"
High-level event format

<event>
    <min_date_time>1291573279.718</min_date_time>
    <max_date_time>1291573279.718</max_date_time>
    <evidence_source>CH-Smythe-01</evidence_source>
    <description>Google Search for 'pdf creator'</description>
    <category>Web</category>
    <device>CH-Smythe-01</device>
    <type>Google Search</type>
    <files></files>
    <summary></summary>
    <trigger_evidence_artefact>
        <reasoning_artefact>
            <description>Google search URL found in /Documents and Settings/Alan/Local Set</description>
            <id>42117</id>
            <test_event>
                <low_event>
                    <type>URL Visit</type>
                    <path>http://(\.+\.)(google)\.[A-z]{2}.*/(.+)</path>
                </low_event>
            </test_event>
        </reasoning_artefact>
    </trigger_evidence_artefact>
    <key name="URL">http://www.google.co.uk/search?hl=en&source=hp&q=pdf+creator&meta=&aq=
    <key name="Search_Term">pdf creator</key>
    <key name="Browser">IEExplorer</key>
</event>
Supporting and contradictory artefacts

<supporting_artefacts>
  <reasoning_artefact>
    <description>InstallDate artefact found in Registry</description>
    <id>553204</id>
    <test_event>
      <low_event>
        <plugin>Registry Parser</plugin>
        <path>{}/Microsoft/Windows NT/CurrentVersion$</path>
        <key name="InstallDate">.*</key>
      </low_event>
    </test_event>
  </reasoning_artefact>
</supporting_artefacts>

<contradictory_artefacts>
  <reasoning_artefact>
    <description>Windows Folder created not found at similar time</description>
    <id>-1</id>
    <test_event>
      <low_event>
        <plugin>Mounted File System</plugin>
        <type>Created</type>
        <path>^Windows$</path>
      </low_event>
    </test_event>
  </reasoning_artefact>
</contradictory_artefacts>
High-level event format

(event
  <min_date_time>1291579906</min_date_time>
  <max_date_time>1291579906</max_date_time>
  <evidence_source>CH-Smythe-01</evidence_source>
  <description>panther.pdf created</description>
  <category>User Activity</category>
  <device>CH-Smythe-01</device>
  <type>PDF created</type>
  <files>
    <file>
      <original_file>/Documents and Settings/Alan/Desktop/panther.pdf</original_file>
      <copied_file>CH-Smythe-01_0000000A.pdf</copied_file>
    </file>
  </files>
  <summary></summary>
  <trigger_evidence_artefact>
    <reasoning_artefact>
      <description>Created time for .pdf file panther.pdf in /Documents and Settings/Alan/Desktop/</description>
      <id>329</id>
      <test_event>
        <low_event>
          <type>Created</type>
          <path>.*\.pdf$</path>
        </low_event>
      </test_event>
    </reasoning_artefact>
    <trigger_evidence_artefact>
      <key name="File Size">39880</key>
      <key name="File Name">panther.pdf</key>
      <key name="File Path">/Documents and Settings/Alan/Desktop/panther.pdf</key>
    </trigger_evidence_artefact>
  </trigger_evidence_artefact>
)</event>
Case folder structure

- config.txt
- data
- extracted
- high_timelines
- logs
- low_timelines
Results
## Performance

**Table 1**

Example times for timeline generation and analysis. The first is from a small, test VM, others are from ‘real world’ systems.

<table>
<thead>
<tr>
<th>Volume size</th>
<th>Approx. time system in use</th>
<th>Low-events produced</th>
<th>Time for low generation (hh:mm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 GB</td>
<td>2 months</td>
<td>0.6 million</td>
<td>0:15</td>
</tr>
<tr>
<td>100 GB</td>
<td>2 years</td>
<td>1.2 million</td>
<td>0:42</td>
</tr>
<tr>
<td>250 GB</td>
<td>5 years</td>
<td>1.6 million</td>
<td>1:05</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Volume size</th>
<th>Number of analysers</th>
<th>High-events produced</th>
<th>Time for analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 GB</td>
<td>19</td>
<td>666</td>
<td>0:28</td>
</tr>
<tr>
<td>100 GB</td>
<td>19</td>
<td>2704</td>
<td>1:10</td>
</tr>
<tr>
<td>250 GB</td>
<td>17</td>
<td>3902</td>
<td>1:14</td>
</tr>
</tbody>
</table>
Visualising high-level timelines using Timeflow
## User Activity

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>:50</td>
<td>USB device connected (E:/)</td>
</tr>
<tr>
<td>:51</td>
<td>Word document created (/Users/gordon/Documents/hack–wifi.docx)</td>
</tr>
<tr>
<td>:52</td>
<td></td>
</tr>
<tr>
<td>:53</td>
<td></td>
</tr>
<tr>
<td>:54</td>
<td></td>
</tr>
<tr>
<td>:55</td>
<td></td>
</tr>
<tr>
<td>:56</td>
<td></td>
</tr>
<tr>
<td>:57</td>
<td></td>
</tr>
</tbody>
</table>

**Feb 15 2012 13:00**
Visualising high-level timelines using d3.js
(work in progress)
d3.js used to show high and supporting low-level events

### High Level Event Details

- **event_id**: 1467
- **min_date_time**: Sat Mar 26 2011 08:19:51 GMT-0400 (EDT)
- **max_date_time**: Sat Mar 26 2011 08:19:51 GMT-0400 (EDT)
- **evidence_source**: HC-TechCom
- **description**: Shutdown time
- **category**: System
- **device**: HC-TechCom
- **type**: Shutdown time

### Low Level Event Details

- **id**: 397081
- **min_date_time**: Sat Mar 26 2011 08:19:51 GMT-0400 (EDT)
- **max_date_time**: Sat Mar 26 2011 08:19:51 GMT-0400 (EDT)
- **evidence**: HC-TechCom
- **plugin**: Registry Parser
- **type**: Last Updated
- **path**: CMI-CreatHive(3D971F19-49AB-4000-8D39-A5D9C673B809)/Microsoft/Windows/CurrentVersion/Reliability/shutdown

**dataprov_source**: Windows/System32/config/SOFTWARE
**dataprov_type**: offset
**dataprov_value**: 4034800

**Keys**:
- **ReasonCode**: 0x000500
- **type**: REG_DWORD
Low-event provides link to raw data
<table>
<thead>
<tr>
<th>ID</th>
<th>Event Details</th>
</tr>
</thead>
</table>

**High Level Event Details**

- **id**: 22
- **min_date_time**: Fri Jul 27 2012 16:50:36 GMT-0400 (EDT)
- **max_date_time**: Fri Jul 27 2012 16:53:12 GMT-0400 (EDT)
- **evidence_source**: JP-Alice_Dylan
- **description**: File Access (Windows/Hid/Cheat.pdf)
- **category**: User Activity
- **device**: JP-Alice_Dylan
- **type**: File Access
- **summary**:
  - Keys:
    - Filename:Cheat.pdf
    - Files:
      - Windows/Hid/Cheat.pdf
      - JPAlice_Dylan_0000012.pdf
  - Supporting:
    - Link file created in Recent Folder
    - /Users/Alice/AppData/Local/Microsoft/Windows/History/History_IE5/MSHist012012072720120728/index.dat
    - Keys:
      - Index_Type: Daily
      - User: Alice
Can show low-level events that occurred at a similar time

<table>
<thead>
<tr>
<th>User</th>
<th>Time</th>
<th>Event Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>JP-Alice_Dylan</td>
<td>Fri Jul 27 2012 16:45:12 GMT-0400 (EDT)</td>
<td>Web Visit to '127.0.0.1'</td>
<td>Web Visit</td>
</tr>
</tbody>
</table>

**files:**
- Windows/Hid/Cheat.pdf:
  - JM-Alice_Dylan_00000012.pdf

**supporting:**
- Link File created in Recent Folder
  - (\Users\Alice\AppData\Roaming\Microsoft\Windows\Recent\HidLink):
    - 44932
- Mounted File SystemMFT Created
  - (\Users*,\AppData\Roaming\Microsoft\Windows\Recent\{}(\*\)?.lnk)
- Recent from Index.dat (\file://C:\Windows\Hid\Cheat.pdf):
  - 221314
- Explorer Parser: URL Visits Windows\Hid\Cheat.pdf:
  - 225094
- Recent from Index.dat (\file://C:\Windows\Hid\Cheat.pdf):
  - 223114
- Explorer Parser: URL Visits file://(\A-z\{1\}:)/(\+/(-((\A-z\{3\})))))
  - 225094
- Recent from Index.dat (\file://C:\Windows\Hid\Cheat.pdf):
  - 223114
- Explorer Parser: URL Visits file://(\A-z\{1\}:)/(\+/(-((\A-z\{3\})))))
  - 225094
- Recent from Index.dat (\file://C:\Windows\Hid\Cheat.pdf):
  - 223114
- Explorer Parser: URL Visits file://(\A-z\{1\}:)/(\+/(-((\A-z\{3\})))))
  - 225094
Evaluation (1)

- Demonstrated as a feasible approach
- Provenance can be preserved
- Performance-wise ok, and can be improved
- Implementation:
  - Gaps in extractor scope (notably evtx)
  - Supporting and contradictory should be automatically added
  - Analyser scripts need some simplification
Evaluation (2)

- High-level event format is only loosely evaluated with useful examples
- Taxonomy of event types and categories
Future Work

• More extractors including importing from other tools
• More complex analysers
• Testing
• Parallel processing
• Cross-drive analysis
• Evaluation of high-level and low-level timelines
• Visualisations
Questions?

Dr Chris Hargreaves
Lecturer
Centre for Forensic Computing
Cranfield University
Defence Academy of the UK
Shrivenham, UK

c.j.hargreaves@cranfield.ac.uk

Jony Patterson
Research Fellow
Centre for Forensic Computing
Cranfield University
Defence Academy of the UK
Shrivenham, UK

j.patterson@cranfield.ac.uk