

# The Undiscovered Country - Device Presence Estimation from Home Router Memory Dumps

Tobias Fiebig

University of Amsterdam

07/04/2013

# The Situation



- *Who* has *when* been *where* is an important question during an investigation.
- **Example:** One wants to establish that a murder suspect visited the victims home on a specific date.
- People tend to carry all sorts of wireless and network capable devices *with* them.
- Nearly everywhere where there is Internet there is a small home router.

# Router?





- Small device handed out by Internet Service Providers to a customer - enables the customer to have more than one device on the Internet.
- Mostly MIPS or ARM based.
- Cheap Design - Exposed JTAG ports are very common.
- Usually “manages” the local network, usually with RFC1918 and DHCP.

# DHCP?



- *State-full* protocol to manage IPv4 address assignments.
- State has to be kept somewhere.
- Can not do it in flash - memory file-system here we come!

# JTAG?



- Standardized debug interface for most embedded CPUs.
- Allows direct access to device memory.

# Research Question



Is it possible to extract DHCP state information from a home routers memory and establish a time-line of device presence with this information in a forensically sound manner?

# Forensic Requirements



Am forensically sound memory image extraction method has to have the following features [Vömel & Freiling, 2012]:

**Correctness and Completeness**: Everything that has been read was read as it was in the memory and nothing that has not been in that memory is read and everything that is read is written to the dump-file as it was read.

**Atomicity**: If memory area $A$ is read at time $t$, all subsequent ones have to be read in the state they had at $t$.

**Integrity**: The method does not change the memory contents before reading them.

# Forensic Verification



Furthermore the following verification techniques should be applied to the technique:

**Self-similarity check**: Check for self-similarity using dotplots, following the method of [Inoue *et al.*, 2011] to verify correctness.

**Integrity check**: Check if two subsequent extraction processes on the same target produce highly identical images and ensure that no transmission errors occure.

# Hardware



- Experiments have been performed with a TP-Link 1043ND.
  - Small MIPS based device.
  - Readily available in the lab.
  - Well documented.
  - Nicely exposed JTAG port.

# Method - Overview



The method itself consists of five steps, each one catering to some of the forensic requirements.

- Plug-in the JTAG Cable
- Connect patched OpenOCD
- Halt the CPU
- Extract memory
- Analyze the image

# Plug-in the JTAG Cable





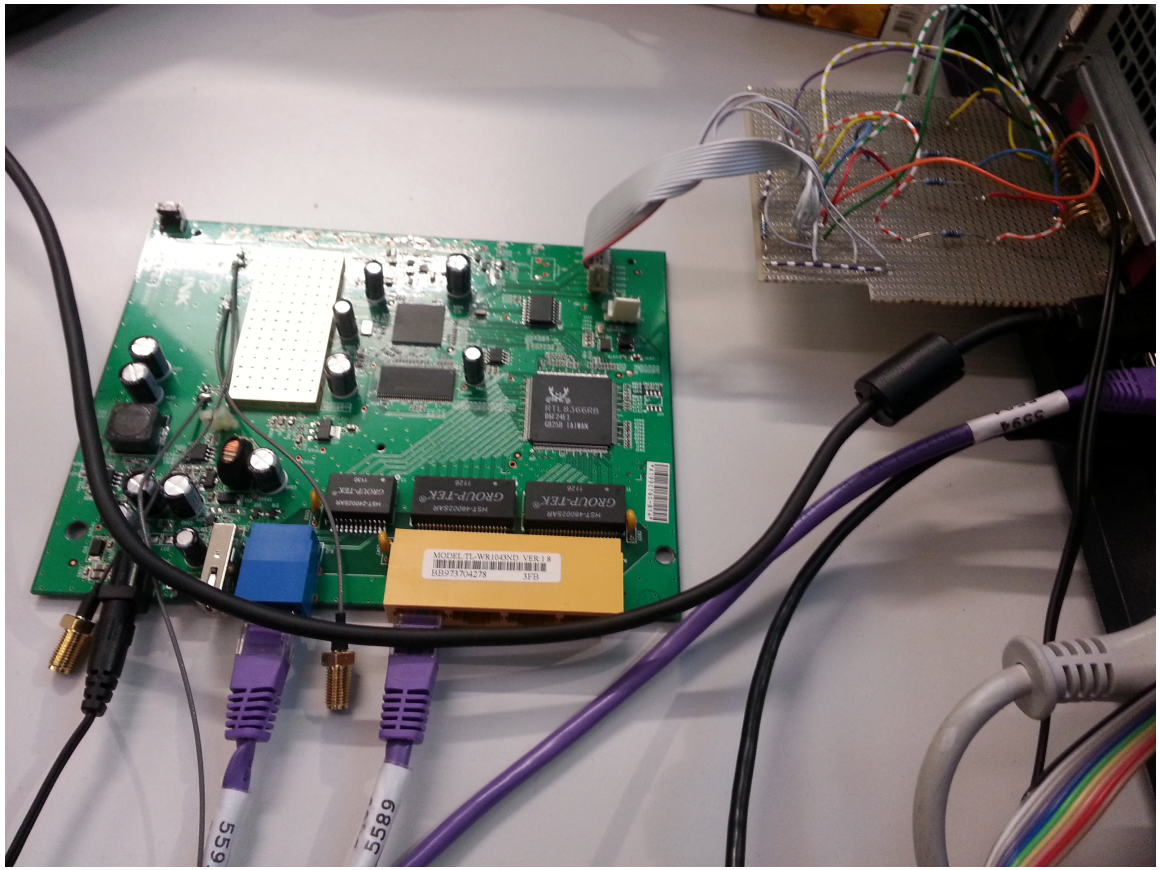

Figure: A DLC5 Cable is used to connect a TP-Link 1043ND with a standard PC.

# Plug-in the JTAG Cable



- Use of “dumb” cable reduces probability of tainted correctness due to operations on the cable.

# Connect OpenOCD



- A tool for interacting with devices via JTAG.
- Not developed for forensics, but made so it "[...] never displays wrong or inaccurate information" [Rath, 2008, p. 38].
- Patched to directly access the memory instead of using the processor's MMU - eliminates further issues for the correctness.
- Should not perform any operations in the Target memory.

# Halt CPU



- Stops all execution in the CPU.
- Ensures atomicity - where there is no computation, there is no change.

# Extract Memory



- Tell OpenOCD to get the memory...
- ... then mostly wait. Speed: 0.66KiB/s
- Takes roughly 12h for a 32MB image.

# Analysis



- Lease-file on 1043ND is not as plain-text in the RAM but in the DHCP servers memory structures.
- As available tooling has no MIPS support: Focus on log-messages containing the same information.
- Create a tool that extracts time-lines and creates visualizations.

# Test-Setup



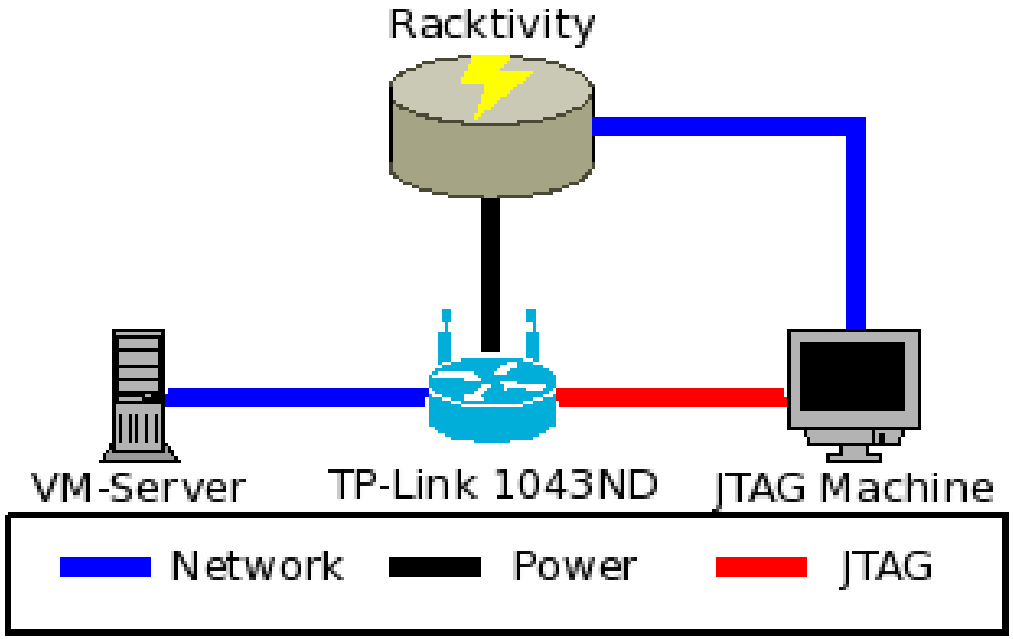


Figure: Schematic representation of the setup used for testing the proposed method.

# Simulated Scenarios



Performed extractions on the device after simulating seven different scenarios.

| Scenario | Description |
|---|---|
| adv-test-1-4 | boot 1 host, shutdown, wait 4h, dump memory |
| adv-test-1-8 | boot 1 host, shutdown, wait 8h, dump memory |
| adv-test-8-4 | boot 8 hosts, shutdown, wait 4h, dump memory |
| adv-test-8-8 | boot 8 hosts, shutdown, wait 8h, dump memory |
| plain-test-4 | boot 4 hosts, dump memory |
| plain-test-8 | boot 8 hosts, dump memory |
| complex | boot 3 hosts, wait 1.25h, boot 3 hosts, shutdown 2 hosts, wait 12h, dump memory |

Table: Overview of the simulated scenarios.

# Image Validation



- In addition to these scenarios, the previously mentioned subsequent extraction from the same target state was performed. The extracted images were bit-wise identical. This indicates a high integrity of the method and no introduction of random errors during the transfer.
- The creation of a dotplot with the method described by [Inoue *et al.*, 2011] indicated no significant self-similarities that would yield a tainted image.

# Image Validation



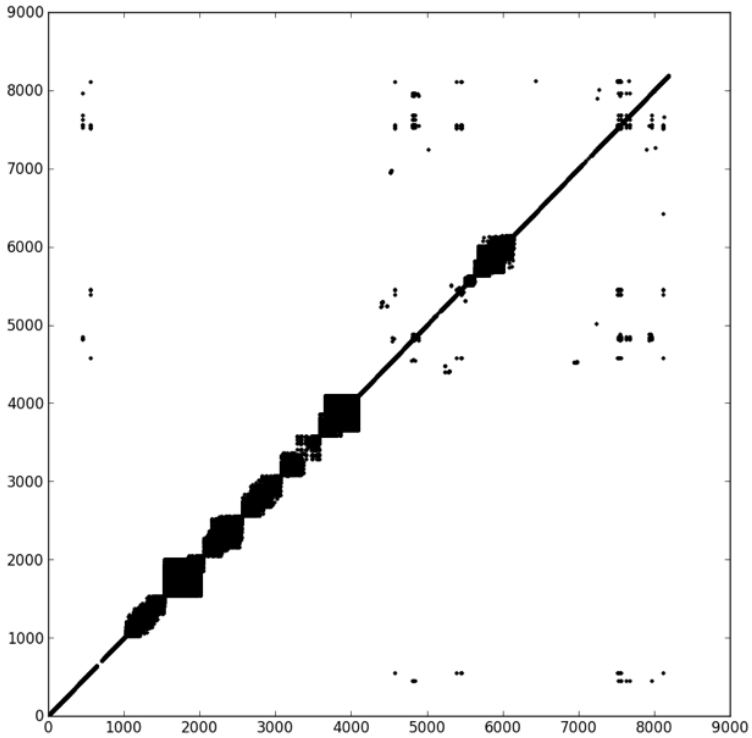


Figure: Dotplot showing self-similarity between pages in a memory image obtained by the author. The axis show the index of the corresponding pages.

# Result Metrics



- Amount of correctly detected host presences.
- Correctly detected join-times.
- Hosts that could be found in the DHCP Server memory.
- Hosts that were detected but were not actually present.

# Results



| Scenario | Detection Rate | Accuracy | Hosts In-Memory | False Positives | Total Hosts |
|---|---|---|---|---|---|
| adv-test-1-4 | 1 | 1 | 1 | 0 | 1 |
| adv-test-1-8 | 1 | 1 | 1 | 0 | 1 |
| adv-test-8-4 | 2 | 2 | 8 | 0 | 8 |
| adv-test-8-8 | 2 | 2 | 8 | 0 | 8 |
| plain-test-4 | 4 | 4 | 4 | 0 | 4 |
| plain-test-8 | 8 | 8 | 8 | 0 | 8 |
| complex | 6 | 3 | 6 | 0 | 6 |

Table: Results for the seven scenarios in the three different metrics.

# Example - Complex Test Visualization




Rel. Time t since device boot ( in seconds )
Green: Host up; Red: Host down;


Rel. Time t since device boot ( in seconds )
Black/Gray: Handed out leases, darkness determines certainty of presence Red: Requests Only

# Conclusion



So: Is it possible to extract DHCP state information from a home routers memory and establish a timeline of device presence with this information in a forensically sound manner?

- In general: Yes.
- The memory extraction method is sound.
- The presence of a certain device can be established.
- Rollover effects make the creation of timelines more difficult but not impossible.
- Further research has to be performed on the extraction of in-memory MAC addresses and lease-files.
- Possible effects of cosmic ray induced soft-errors have not been taken into account, see [Tosaka *et al.*, 2008].

# Further Work



- Investigate the method on more home router devices.
- Explore other interesting data-sources in home router memory, e.g. networking related structures (e.g. [Beverly *et al.*, 2011]) and more.
- Investigate the impact of cosmic rays.
- Improve the support for the MIPS architecture in existing memory analysis tooling.



Beverly, Robert, Garfinkel, Simson, & Cardwell, Greg. 2011.
Forensic carving of network packets and associated data structures.
*Digital Investigation*, **8**, S78–S89.

Inoue, Hajime, Adelstein, Frank, & Joyce, Robert A. 2011.
Visualization in testing a volatile memory forensic tool.
*Digital Investigation*, **8**, S42–S51.

Rath, Dominic. 2008.
*Open On-Chip Debugger*.

Tosaka, Yoshiharu, Takasu, Ryozo, Uemura, Taiki, Ehara, Hideo, Matsuyama, Hideya, Satoh, Shigeo, Kawai, Atsushi, & Hayashi, Masahiko. 2008.
Simultaneous measurement of soft error rate of 90 nm cmos sram and cosmic ray neutron spectra at the summit of mauna kea.
*Pages 727–728 of: IEEE International Reliability Physics Symposium, 2008. IRPS 2008.*
IEEE.

Vömel, Stefan, & Freiling, Felix C. 2012.
Correctness, atomicity, and integrity: Defining criteria for forensically-sound memory acquisition.
*Digital Investigation*, **9**(2), 125–137.