FOX IT
part of nccgroup

Dissect: An incident response game-changer

A streamlined, easy-to-use solution, now available as Open Source Software

Level up your incident response capabilities

As our online and offline worlds intertwine further, cyber incidents have a greater impact. Whether it's employee fraud or a nation state attack, they're becoming evermore complex and sophisticated, as are the IT systems on which they take place. The main question for the good guys is:

How do you scale incident response capabilities, while maintaining or even improving efficiency and accuracy during investigation?

The solution: Dissect

Dissect enables the acquisition and analysis of hundreds to thousands of systems in a matter of hours – a game-changer for incident response teams. Its modular approach means anyone with Python experience can use the concise API to adapt it to their own needs and create output to connect it to the platform of their liking. And the best part is, it's now available as Open Source Software.

Why will you benefit from Dissect?

1. **Respond rapidly to complex attacks**
   In essence, incident response still comes down to an organization experiencing pain from insiders, spies, or criminals, and calling a trusted third party to make the pain go away.

   This seems straightforward, but incident response is a machine with many changing parts. Attackers nowadays aim to take over a complete infrastructure, often with both on-premise and cloud systems. This requires incident response teams to investigate more systems and reconstruct longer timelines with more diverse events than in the past. With all this, plus additional time pressure, incident handling is more complex than ever.

   Dissect helps ease this complexity by enabling analysis of thousands of systems in hours, and looking for data in known or configured locations, without parsing every file on a disk. This drastically improves performance and is sufficient for most IR engagements. If during initial triage it turns out more analysis is required, you can always fall back to the more traditional toolset for individual system analysis.

2. **Go beyond current capabilities**
   Many incident response engagements have one thing in common: a large, complex infrastructure that needs careful examination for Indicators of Compromise (IOCs), while the investigators may need to remain undetected by sophisticated threat actors. These cases often go beyond the capacities of commonly used analysis tools.

3. **Keep standards high at all times**
   There's no shortage of parsers and tools for DFIR tasks that work fine most of the time. But whether it's missing functionalities, automation difficulties or poor performance, 'most of the time' simply isn't good enough.

4. **Unlock a seamless experience**
   While many tools perform similar tasks, their output format, e.g. CSV, JSON or Excel, can differ wildly. Besides making it harder to collaborate, the choice of tools could lead to different findings, which is detrimental to the quality of any engagement. On top of that, the plethora of tools makes it hard to automate tasks in an analysis pipeline.

5. **Take control at any scale**
   Nowadays, there's a need for swift analysis or at least an initial impression of the state of hosts within hours from the moment of acquisition. Most current tools aren't made with this goal in mind.

   Dissect puts you in control of your entire analysis chain as it is easy to expand with different implementations of various parsers. This lets you reuse useful components, not limiting them to the capabilities of a single script. You can also easily add exotic systems without making changes to the rest of the framework. This flexibility enables you to easily create new and exciting capabilities with Dissect, like adding hypervisor-based data acquisition, which allows for system analysis without detection by the compromising threat actor.

6. **Ready for state actors**
   Especially when dealing with advanced threat actors, you want to be as stealthy as possible. An example of how Dissect can help with this is by allowing data acquisition from a hypervisor, which allows for analysis of a virtual machine without the threat actor who compromised the virtual machine detecting it. Dissect can also bypass any lock the hypervisor might have on a virtual disk, without running the risk of data corruption. Another example is that the Acquire data acquisition tool, when executed on live systems, reads straight from the raw disk, not using operating system APIs to copy files. This limits the possibilities for threat actors to tamper with the evidence collection.

An enterprise-scale forensics framework for data acquisition and analysis

Years ago, Fox-IT saw an opportunity to bring its technical incident response capabilities to the next level. We decided to develop new in-house tooling for high-performance enterprise forensics, as there were no such tools available that fitted our needs. This was the start of Dissect.

The philosophy behind Dissect

Abstraction layers are the core of the framework. On systems, concepts like users, network interfaces, and services are ubiquitous. Concepts such as disks, volumes, filesystems and operating systems offer abstraction opportunities. With the right combination of abstraction layers, information can be accessed universally, wherever the data is held.

There are a lot of repetitive steps to take before even starting the analysis on a host. These are all opportunities for automation, just think of the number of third-party tools used, and how each of these steps is susceptible to technical, process, and scalability limitations.

Dissect consists of five core abstraction layers:

- Containers
- Volumes
- Filesystems
- Operating systems
- Analysis plugins

Each layer is flexible and can operate independently from the others. On top of the basic layers are plugins responsible for ensuring an operating system is properly loaded. Finally, there are analysis plugins. These can include OS-specific plugins, like for Windows event logs, Linux bash history, or more generic plugins, like browser history or filesystem timelining. Combined, these layers allow interaction with any type of source data.

The most important benefit of this layered approach is that analysis plugins are abstracted away from your source data. With this 'write once, run anywhere' approach, tools are no longer limited to a single-data format or platform, but instead are data format agnostic. Analysts therefore no longer need to worry about how to access investigation data, and can instead focus more on performing actual analysis.

Making the world safer and more secure

Dissect has pushed our own incident response practice capabilities. We want to share this with the world to make it a safer, more secure place.

With increased usage we expect valuable input into the framework from other members of the security community.

Although outstanding tools always help, we know we can only deliver effective incident response thanks to our experienced, talented team.

For more detailed information about Dissect, please go to **fox-it.com/nl-en/dissect/**
Or if you need assistance, contact our hotline any time at **fox-it.com/nl/cyber-incident-response/** and our world-class incident responders will be happy to help.

About Fox-IT

It's a new era of risk. Defy it with Fox-IT's end-to-end cyber security and resilience solutions, and confidently embrace technology to support sustainable growth and success.

From governments to tech giants, financial institutions to expanding businesses, for over 30 years we have proudly provided them all with strong security solutions. And with a worldwide team of over 2,400 experts we're ready to do the same for you.

With Fox-IT, part of NCC Group, you take your business to the next level. Unleash innovation without the obstacle of cyber threats.

For more detailed information about Fox-IT, including partner details, please go to **fox-it.com**