FOX IT
part of nccgroup

Dissect

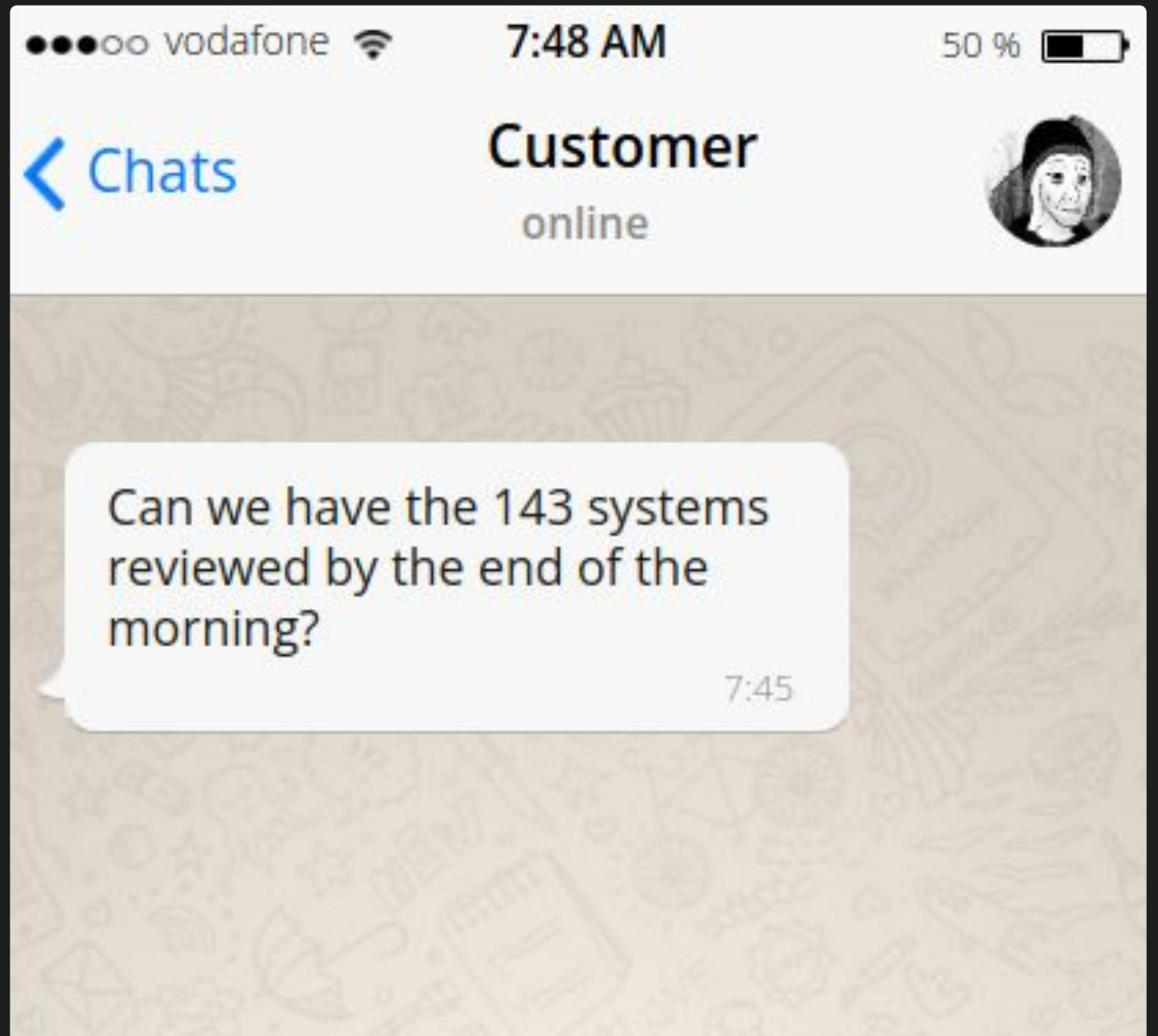
The Solution to Large-Scale Incident Response

(and why APTs hate us!)

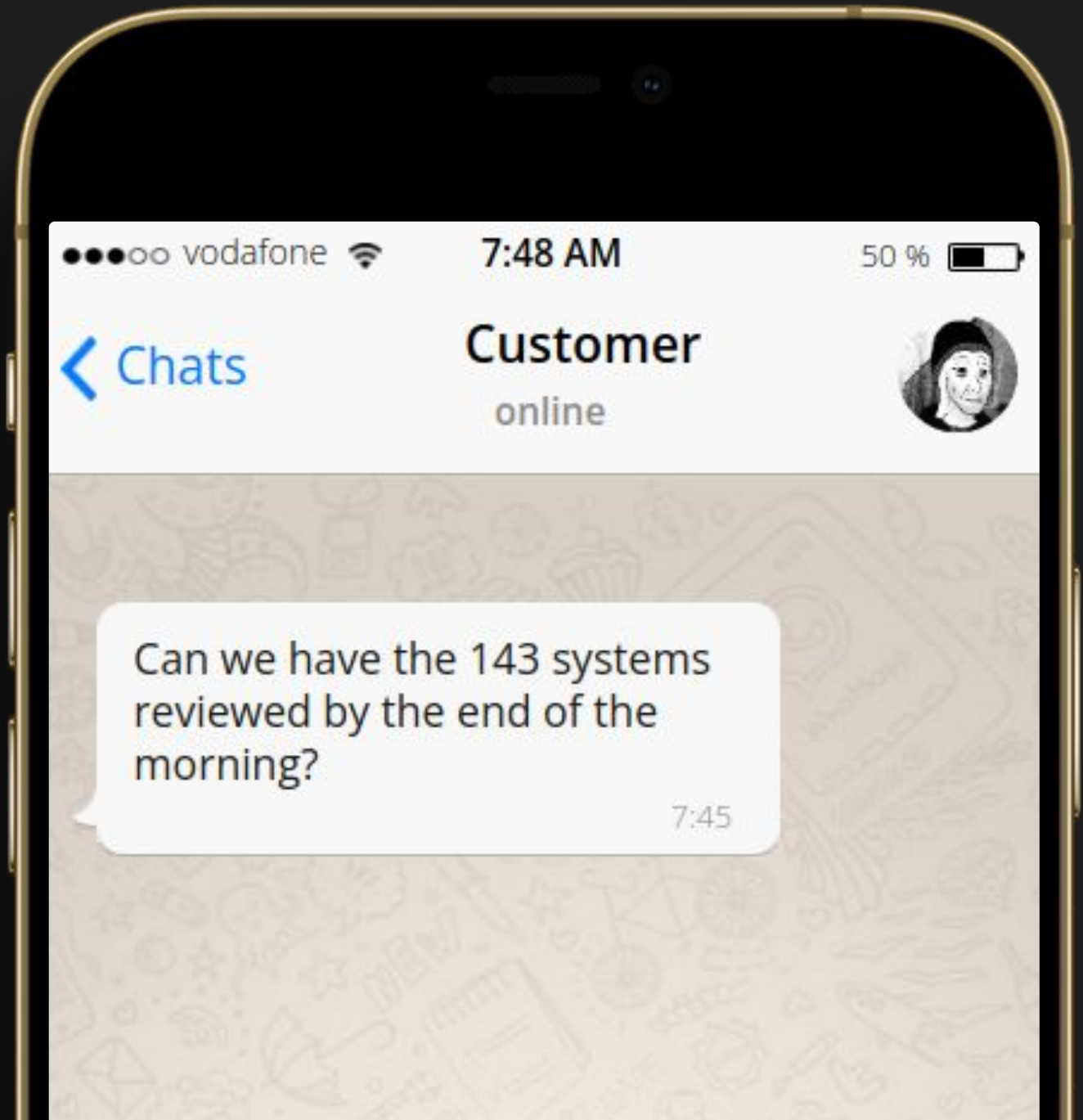
Erik Schamper — Security Researcher

Willem Zeeman — Incident Handler

2023-06-05 TLP:CLEAR



FOX IT
part of nccgroup



FOX IT
part of nccgroup

```
$ target-query -f <artefact> /systems/*
```

```
$ target-query -f <artefact> /systems/*
```

FOX IT
part of nccgroup

$

activitiescache adpolicy alternateshell amcache anydesk apache appinit apt architecture atop audit auditpol authlog bam bashhistory bootshell btmp caddy catroot chrome cim cit clfs clsid codepage commandhistory cronjobs defender docker domain dpkg edge notifications etl evt evtx exchange filerenameop firefox firewall hostname yum icat iexplore iis install_date keyboard knowndlls language lastlog lnk mcafee messages mft mft_timeline mru muicache ndis network_history nginx ntversion nullsessionpipes pathenvironment zypper path_extensions pfro powershell_history prefetch recentfilecache recyclebin runkeys sam securelog services sessionmanager sevenzip shellbags shimcache sru ssh startupinfo suid_binaries syscache syslog tasks teamviewer thumbcache timezone trendmicro trusteddocs ual usb userassist usnjrnl walkfs wer winrar wireguard wtmp yara

activitiescache adpolicy alternateshell amcache anydesk apache appinit apt architecture atop audit auditpol authlog bam bashhistory bootshell btmp caddy catroot chrome cim cit clfs clsid codepage commandhistory cronjobs defender docker domain dpkg edge notifications etl evt evtx exchange filerenameop firefox firewall hostname yum icat iexplore iis install_date keyboard knowndlls language lastlog lnk mcafee messages mft mft_timeline mru muicache ndis network_history nginx ntversion nullsessionpipes pathenvironment zypper path_extensions pfro powershell_history prefetch recentfilecache recyclebin runkeys sam securelog services sessionmanager sevenzip shellbags shimcache sru ssh startupinfo suid_binaries syscache syslog tasks teamviewer thumbcache timezone trendmicro trusteddocs ual usb userassist usnjrnl walkfs wer winrar wireguard wtmp yara

Make the data fit you

```
$ target-query ... \
  | rdump -w json://
```

Make the data fit you

```
$ target-query ... \
    | rdump -w csv://
```

Make the data fit you

```
$ target-query ... \
| rdump -w splunk://<ip>:1337
```

Make the data fit you

```
$ target-query ... \
| rdump -w elastic://<ip>:1337
```

No matter the format

No matter the amount

No boring manual steps

Just investigate

```
$ pip install dissect
```

fox-it/dissect

FOX IT
part of nccgroup

This is Dissect

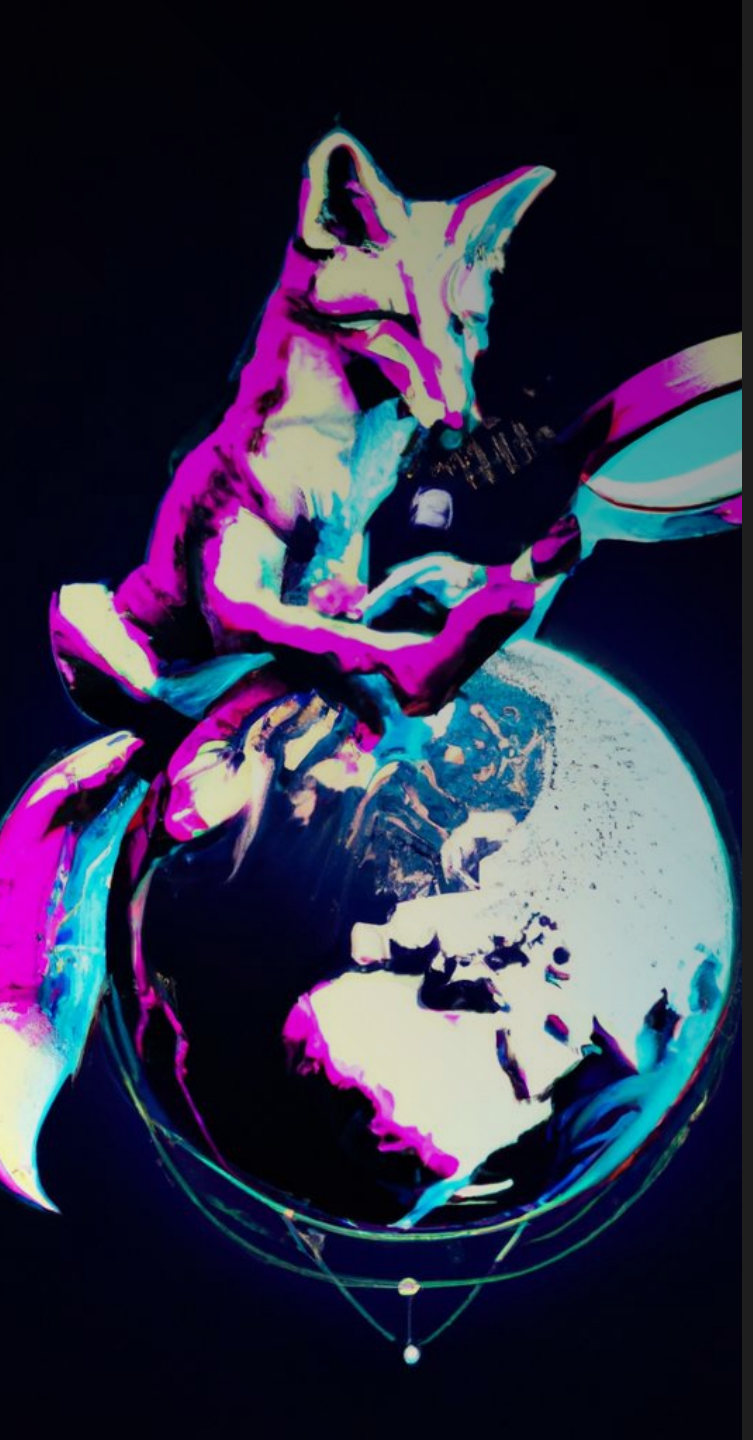
- Modular pure Python framework
  - Contains libraries and analyst tooling
  - 20+ libraries
  - The magic: dissect.target
  - 100+ parsers and plugins

- Based on a decade of IR and development

FOX IT
part of nccgroup

But why?

- Created to solve tough challenges
  - Thousands of systems? No problem
  - No data and actor beyond our reach
  - Team distribution doesn’t matter
- Zero compromise on flexibility
- Open-source? For a more secure society!



Not just for analysis

- We created Acquire for data collection
- Generates small forensic packages
- Works on Windows, Linux and ESXi
  - Guests on ESXi
- Already have investigation data?
  - Works on everything Dissect supports

FOX IT
part of nccgroup

Some numbers 💪

- ~ 100 systems is common
  - Only requires 1 host analyst a few days
- Investigation with 250k+ source items
  - 2 host analysts and 2 log analysts for 3 weeks

FOX IT
part of nccgroup

Zero compromise

- Exotic backup or disk format?
  - Write a new parser

```
dissect
└── hypervisor
    ├── backup
    │   ├── ova.py
    │   ├── vbk.py
    │   ├── vma.py
    │   ├── wim.py
    │   └── xva.py
    ├── descriptor
    │   ├── hyperv.py
    │   ├── ovf.py
    │   ├── pvs.py
    │   ├── vbox.py
    │   └── vmx.py
    └── disk
        ├── hdd.py
        ├── qcow2.py
        ├── vdi.py
        ├── vhd.py
        ├── vhdx.py
        └── vmdk.py
```

Zero compromise

- Partially encrypted data?
  - Write a loader to for the plain text data

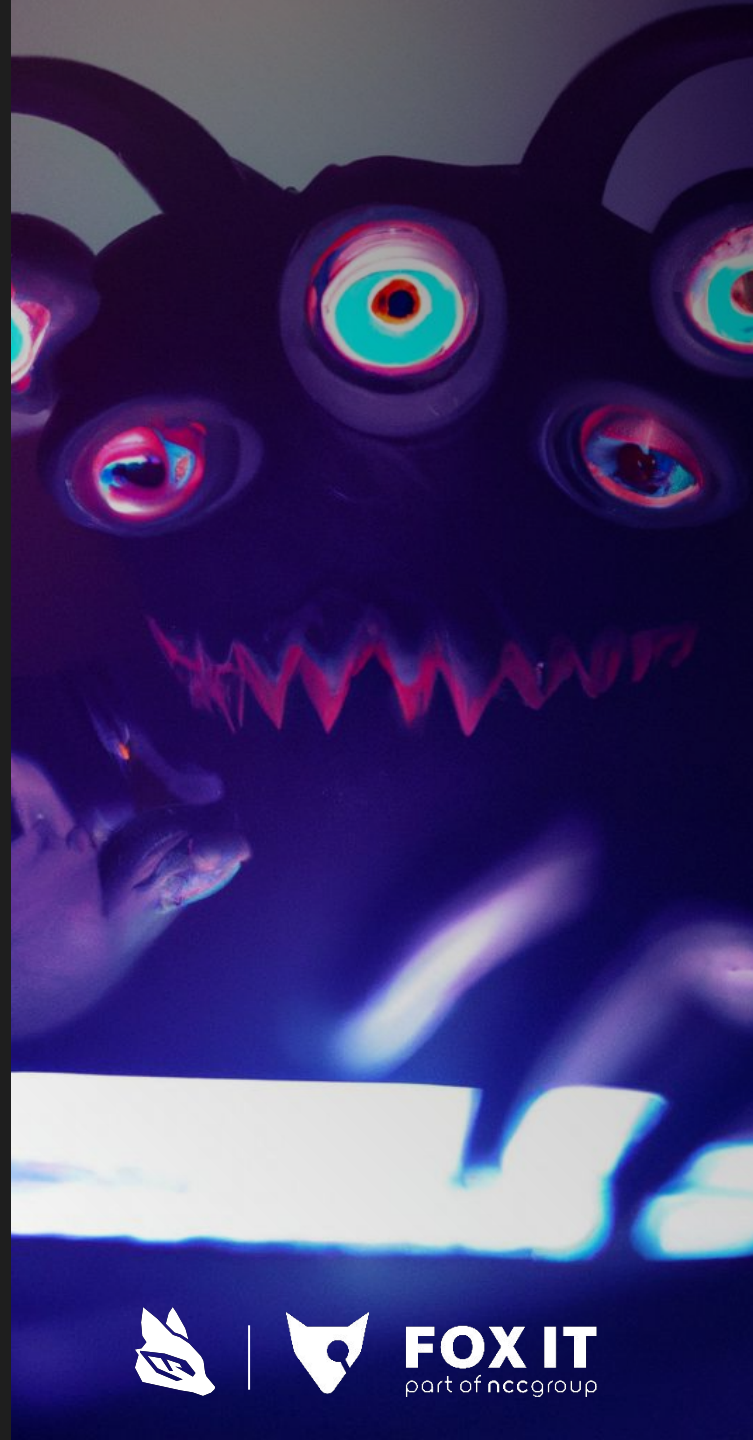
```
for needle, offset in scrape_pos(fh, FS_NEEDLES):
    cur_seek = fh.tell()

    try:
        if needle == NTFS_NEEDLE:
            volume = stream.RelativeStream(fh, offset)
            fs = filesystem.open(volume)
            size = fs.ntfs.sector_count * fs.ntfs.sector_size
        elif needle == EXTFS_NEEDLE:
            volume = stream.RelativeStream(fh, offset - EXTFS_NEEDLE_OFFSET)
            fs = filesystem.open(volume)
            size = fs.extfs.block_count * fs.extfs.block_size

        target.filesystems.add(fs)
        target.fs.mount(f"fs{fs_idx}", fs)
        fs_idx += 1

        fh.seek(offset + size)
    except Exception:
        fh.seek(cur_seek)
```

FOX IT
part of nccgroup

Zero compromise

- Unknown or low-level malware traces?
  - Use the Dissect API to dig deeper

```
In [1]: t.hostname
Out[1]: 'dissect-centos'

In [2]: t.version
Out[2]: 'CentOS Linux 8'

In [3]: t.fs.path("/etc/hosts").read_text()
Out[3]: '127.0.0.1   localhost localhost.localdomain localhost4 localhost4.lo
caldomain4\n::1         localhost localhost.localdomain localhost6 localhost6
.localdomain6\n'

In [4]: from dissect.cstruct import dumpstruct

In [5]: dumpstruct(t.filesystems[1].get("/etc/hostname").entry.inode)

00000000  49 4e 81 a4 03 02 00 00  00 00 00 00 00 00 00 00  IN..............
00000010  00 00 00 01 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000020  64 47 8b 1f 3a 60 bc 6c  64 47 97 e9 13 1b 6f 80  dG..:`.ldG....o.
00000030  64 47 97 e9 13 1b 6f 80  00 00 00 00 00 00 00 1b  dG....o.........
00000040  00 00 00 00 00 00 00 01  00 00 00 00 00 00 00 01  ................
00000050  00 00 23 01 00 00 00 00  00 00 00 00 b2 53 39 d2  ..#..........S9.
00000060  ff ff ff ff f5 6d 20 0e  00 00 00 00 00 00 00 09  .....m ..........
```

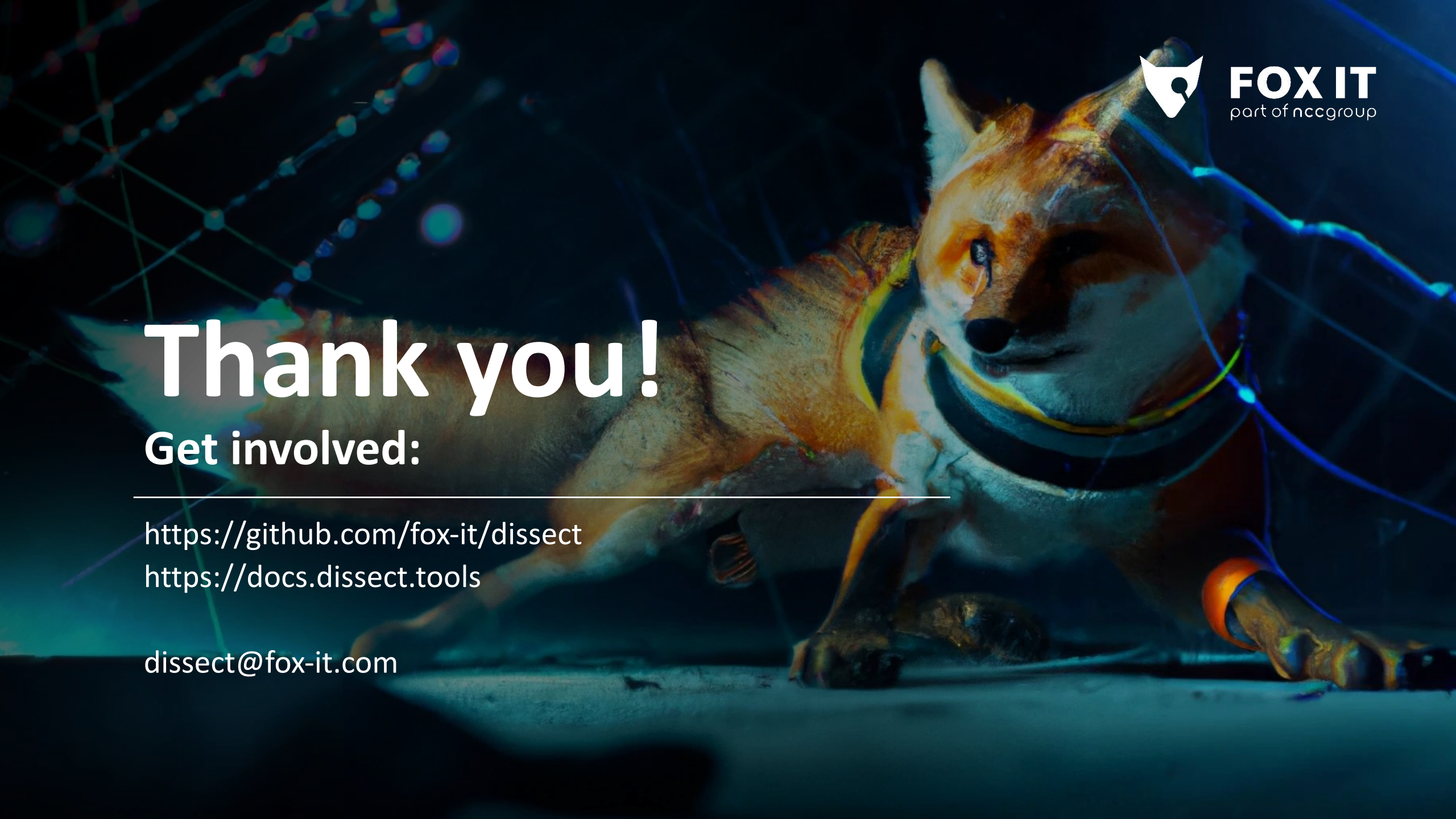


Takeaways

- Dissect as your central processing framework
- Reusability of tools on any source material
- Dig deep with the API or use existing tools
- Great help with the FIRST CTF? 😉

- … and more we don’t have time for!
  - Transparent analysis on FDE
  - Hypervisor analysis and acquisition
  - Mobile and appliance analysis

FOX IT
part of nccgroup



Thank you!

Get involved:

https://github.com/fox-it/dissect
https://docs.dissect.tools

dissect@fox-it.com