- Filename: eccouncil-ceh31250-v10-2-1-3-footprinting_pt3.md
- Show Name: CEHv10 (312-50)
- Topic Name: Information Gathering and Vulnerability Identification
- Episode Name: Footprinting Pt.3
- Description: In this episode, Daniel and Zach finish up their exposition on Footprinting. Here they tackle site mirroring, whois searches, DNS reconnaissance, traceroute, and other tools like recon-ng and Maltego.

==

Footprinting Pt.3

- Site Mirroring
    - httrack/webhttrack
    - `wget -mk -w 10 http://bwapp.com/`
- I've heard you talking about network footprinting with "WHOIS"; can you tell us more about that?
    - WHOIS search is used to...
        - Gather Domain info on target
            - Servers
            - Contact info
            - IP info
        - Use `whois`, `dig`, online services
    - DNS info
        - Again, use `dig`
            - Set record type
                - A, NS, MX, PTR, SOA, TXT
    - Holy Grail: ZONE Transfer
        - Sends all DNS info
        - `dig axfr @nsztml.digi.ninja zonetransfer.me`
    - TRACEROUTE
        - Helps map out network devices that connect to target
            - Routers, Firewalls
            - `traceroute itpro.tv`
            - Online tools
    - Other tools
        - **recon-ng**
        - Maltego